Australian Government
Department of Defence
Defence Science and
Technology Organisation

Using Mobile Platforms for Sensitive Government Business

Samuel Chenoweth

Command, Control, Communications and Intelligence Division
Defence Science and Technology Organisation

DSTO-GD-0722

ABSTRACT

Mobile platforms such as smartphones are becoming increasingly popular for both personal and commercial use. When the data being stored and transmitted by these devices is sensitive this can introduce a host of security issues, some of which are discussed in this report. A summary is provided of existing practices for the use of mobile devices with sensitive information, in both governmental and business contexts, and emerging technologies for improving security are reviewed. Finally, some recommendations are offered for policymakers interested in increasing the role that mobile devices are allowed to play within the Australian Public Service and elsewhere.

RELEASE LIMITATION

Approved for public release

Published by

Command, Control, Communications and Intelligence Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 7389 5555
Fax: (08) 7389 6567

AR-015-497
January 2013

APPROVED FOR PUBLIC RELEASE

Using Mobile Platforms for Sensitive Government Business

Executive Summary

This report investigates the issues and risks that are involved when mobile platforms, such as smartphones, are used for conducting sensitive government business. The objective of this work is to develop fresh but well researched perspectives on the manner in which these devices may be used without compromising security, so that policymakers within Defence and elsewhere in Australian government can be better informed when making decisions. The report offers specific advice on how smartphone policies and research efforts may be adjusted to improve smartphone utility in government, better protect confidential information and save on certification costs.

A range of general security issues associated with smartphones are discussed. Additional issues are also identified that arise in specific usage scenarios, namely the traditional corporate technology paradigm where the organisation owns and administers the device and the bring-your-own device paradigm. Some of the known smartphone vulnerabilities are outlined, along with the threats that may exploit these.

A survey of current and emerging smartphone technologies is presented, with a focus of technology for improving smartphone security or facilitating the integration of employee-owned smartphones with corporate or government systems. This survey includes a review of smartphone technology certified for use within the Australian government.

Existing policy and practice for professional smartphone use is reviewed and critiqued, considering the experiences of private industry, the United States Government and the Australian government. Finally, some suggestions are made for how Australian government policy could be improved to provide better utility for professional smartphone users within government, whilst minimising the security risks. Based on technology which is currently available, this report recommends that the present policy of certifying popular commercial smartphone operating systems and allowing users to use personal devices for professional purposes should be reviewed, in favour of forcing users to use a government owned smartphone with a certified hypervisor operating system. Such a system provides secure separation of a number of different enclaves on the phone, which the user may switch between. The advantage of this is that there can be several professional enclaves on the phone, each administered by the organisation and at its own individual classification level, with the operating systems installed and configured by the organisation's information technology staff (e.g. a

previously certified operating system such as Windows Mobile). Moreover, there can also be a personal enclave running an operating system of the employee's choice (e.g. Android), which is fully controlled by the employee and which can become compromised without affecting the security of the other enclaves or the privacy of any sensitive information stored on them.

Some suggestions are also made for areas worthy of future research. In particular, it is recommended that head-mounted audiovisual displays be investigated as a means for allowing the private use of smartphones in public. As an extension of this, it is also proposed that a trusted input / output device be developed, which can allow a user to interact with remote applications on a secure government network, over a virtual private network connection through a personal smartphone and the Internet service provided by the carrier (both of which may be considered to be untrusted).

Contents

Acronyms

2G	Second Generation mobile phones, which are digital but do not include Internet service
3G	Third Generation mobile phones (smartphones), which do include Internet service
802.1x	A wireless communication standard
AES	Advanced Encryption Standard
ARM	a semiconductor and software design company
AT&T	a telecommunications company
AVG	an antivirus software vendor
CCTV	Closed Circuit Television
CIO	Chief Information Officer
CIOG	Chief Information Officer Group
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
DRN	Defence Restricted Network
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
DSTO-RN	Defence Science and Technology Organisation Restricted Network
DVI	Digital Visual Interface
DVG	Digital Video Guard
EAL	Evaluation Assurance Level
EMC	A technology company specialising in information management
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HTC	a manufacturer of smartphones and other mobile devices
ICT	Information and Communications Technology
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INTEGRITY	An operating system kernel developed by Green Hills Software
iOS	Apple's Operating System for mobile devices
IP	Internet Protocol
IT	Information Technology

JLC	Joint Logistics Command
KASUMI	a block cipher scheme
LG	An electronics manufacturer
MAC	Message Authentication Code
MMS	Multimedia Message Service
NFC	Near Field Communication
NIPRNET	Unclassified but Sensitive Internet Protocol (IP) Router Network
NSA	National Security Agency
PC	Personal Computer
PMKeys	A personnel management system used within the Department of Defence
PSPF	Protective Security Policy Framework
PIN	Personal Identification Number
RSA	Rivest Shamir Adleman public key encryption scheme
SIM	Subscriber Identity Module
SIPRNET - Secret Internet Protocol Router Network	
SMS	Short Message Service
TCP	Transmission Control Procol
TEMPEST	a United States research programme into electromagnetic emissions from electronic equipment
TRIODE	TRusted Input Output DEvice
UMTS	Universal Mobile Telecommunications System
USA	United States of America
USB	Universal Serial Bus
VMWare	A software company specialising in virtualisation technology
VPN	Virtual Private Network
WiFi	Wireless Fidelity
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access
WPA2	WiFi Protected Access version 2
WPS	WiFi Protected Setup

1. Introduction

This report investigates the issues associated with the use of mobile devices in an Australian Government context, and suggests policy responses for dealing with them. To that end, this report draws on the experience of both government and private industry in handling such matters. The focus of this report is on smartphones (i.e. third or fourth generation mobile phones), although some of the issues discussed also apply to other mobile devices such as tablets, laptops, etc. Mobile devices other than smartphones are not discussed specifically, and the extent to which issues raised in relation to smartphones may be applied more broadly is left to the reader's judgement.

Section 2 of this report outlines the general security issues associated with smartphone usage, as well as describing some related vulnerabilities and the threats that may exploit them. The contents of that section are applicable to smartphone usage in any context, whether personal, professional or mixed. Section 3 discusses some of the additional issues that arise for smartphone use in a corporate context, where employees may use smartphones for both professional and personal purposes. While these issues are not directly concerned with security, they can have security implications. In Section 4, some emerging technologies for addressing smartphone vulnerabilities and outstanding issues are reviewed. Some existing policies for handling smartphones in government and private industry are reviewed in Section 5, while Section 6 provides recommendations for future policy.

2. General Security Issues, Vulnerabilities and Threats

There is a greater potential for attacks on smartphones than earlier generations of phones, owing to the more complex functionality now available. In effect, a smartphone is an Internet connected PC, and is subject to the same threats that they are. For example, users browsing the web are at risk from cross site scripting attacks when visiting poorly designed websites or could click on links in messages [1] which execute compromising code on the users machine.

Smartphones have additional vulnerabilities that PCs do not have, due to the smartphone's mobility and therefore lower level of physical security; some of these are discussed later in this section. Another important factor is complacency amongst users, who may think of a smartphone as just an upgraded version of an earlier generation phone, and thus do not pay as much attention to its security as they should [2]. The situation has not been helped by the relative immaturity of security technologies for smartphones, due to the newness of the devices and their limited appeal as cybercrime targets during the early days of their introduction [3] when the number of users was relatively low and fragmented between a variety of different types of phone and operating system. More recently, the increasing penetration of smartphones in the mobile phone market and the dominance of Android phones, Blackberries and iPhones [4] means that an exploit developed for just one operating system has the potential to affect a large pool of victims. For this reason, threats to smartphone security are forecast to continue to increase [3]; more attention to security is therefore essential for smartphone users and security professionals alike.

Sections 2.1 to 2.7 discuss issues relating to the major security functions of smartphones, including known vulnerabilities that they have. Other security issues are outlined in Sections 2.8 to 2.12, which are not directly concerned with specific security functions.

2.1 Data Storage Confidentiality

In contrast to older generations of mobile phones, smartphones provide users with the ability to store significant amounts of information and process this using a wide variety of applications. The question then arises as to the privacy of that information in the event that a smartphone is lost, stolen or simply inspected by an unauthorised user. Many older models of smartphone or tablet operating systems (e.g. versions of Android prior to 3.0 [5]) attempted to prevent unauthorised access using a password protected interface only, which can easily be bypassed using a connection to a computer and readily available digital forensics software [6]. A better solution is to encrypt the entire file system, so that the information on the device is unreadable without knowledge of either the encryption key or the password linked to it. Such an approach has been used on the Blackberry for some time [6], and has more recently been introduced to Android 3.0 [7] and the iPhone (3GS) [6]. The effectiveness of such measures is critically dependent on implementation details, however.

An additional layer of protection from stolen data is the ability to sanitise a device prior to disposal or replacement, so that any personal or sensitive information is removed regardless of whether it is encrypted or not. This feature is often able to be activated remotely, in the event that a smartphone is lost or stolen. However, there are ways in which a thief may disable the remote wipe function, such as removing the SIM card [6], removing the battery [8] or blocking signals to the phone using a Faraday cage. The remote wipe feature is thus only useful in situations where the unauthorised custodian of a lost or stolen phone is not intent on stealing data or is unable to disable the feature before the rightful owner has already used it.

2.2 User Authentication

Whether a smartphone uses filesystem encryption or simply attempts to control access to the device, it is important that a reliable method for authenticating users is employed. Traditionally, this is done with a user selected password or PIN. (When filesystem encryption is in use, the master key for the encryption is typically stored in encrypted format itself, using a key derived from the user's password [7]. A change in the user's password then requires only that the file system encryption master key be decrypted with the old password and then encrypted with the new password. If the user's password generated the file system encryption master key directly, it would be necessary to re-encrypt the entire file system.)

Passwords and PINs have a long history of usage and there is a great deal of literature on them for which there is insufficient space to review here. It suffices to say that there are many guidelines available for suitable password policies, such the minimum acceptable length, the need to include mixed case, numerals or special characters, avoidance of dictionary words, limitation of the number of allowed attempts to enter the password, etc. Similar guidelines apply to PINs. It is important for smartphone developers to select password policies that provide adequate assurance of user authentication. Any weaknesses in the policy structure or loopholes that allow users to bypass the normal authentication rules will make the smartphone vulnerable. On the other hand, it is also understood that there is often a trade-off between the security strength of passwords and the ease with which users can remember them, so a policy that is too strict may alienate the developer's user base. In the worst case, stringent password policies could lead an exasperated user to write the password down in a place that is easily associated with the smartphone, such as writing it on a sticker inside the phone's battery housing or writing it on a piece of paper in the user's wallet (which could easily be lost or stolen along with the phone). For these reasons, alternative user authentication methods such as face recognition have been tried, and are discussed further in Section 4.1.

2.2.1 A Case Study – The iPhone 4S

As an example of the complexities of developing appropriate user authentication policies, this report considers the Apple iPhone 4S. Note that the author makes no claims of the iPhone 4S being any more or less secure than alternative smartphones; this case study is included for illustrative purposes only, and some of the vulnerabilities may also be shared by other smartphones. The iPhone is an instructive example since approval has been granted for its limited use within Australian Government (see Section 4.3.4), and in fact DSD's iOS hardening guide [9] (whose implementation is a condition of approval) deals with the vulnerabilities raised in this section.

User authentication on products based on iOS (including the iPhone 4S) is based on just a 4 digit pin by default [10], and it is possible to disable user authentication entirely. Such a short PIN is vulnerable to brute-force guessing, unless there are measures taken to prevent this; in iOS, these measures include locking the phone for one minute after several incorrect PIN entry attempts, increasing the lockout time for subsequent failed attempts, requiring the phone to be connected to the computer it was last synchronised with after a very large number of failed attempts, and the option of configuring the phone to automatically erase itself after 10 failed attempts [11]. While these policies help to make short PINs more secure, they may not prevent successful attacks if users make poor PIN choices. For example, iOS developer statistics show that a set of just 10 different PINs (1234, 0000, 2580=downward traversal of middle column of number pad, 1111, 5555, 5683=LOVE, 0852=upward traversal of middle column of number pad, 2222, 1212, 1998) are in use by 15% of iOS users [12]. Unless special policies are put in place to prevent such simple PINs being selected, then IT managers allowing employees to use their iPhones at work should expect a similar percentage of phones to be vulnerable in this way. The iPhone may be configured to require longer passcodes to be entered, with various options available such as the requirement to include alphabetic characters or special characters [13].

While configuration changes using the iPhone's menu system are acceptable for a security-conscious individual looking to strengthen the phone's security policies, this approach is insufficient for corporate IT departments wishing to maintain security over a fleet of iPhones. Not only is the manual modification of settings tedious and time-consuming, but the configuration changes made can be reversed by the user, potentially creating a security vulnerability. For this reason, Apple has provided the facility to install configuration profiles on iPhones, which are basically an aggregation of various configuration changes that are all applied together when the configuration profile is installed and which cannot be overridden while it is active. It is possible to create configuration profiles that may be removed by the user, that may only be removed if the user enters the passcode associated with the configuration profile, or that cannot be removed at all [13]. (Any configuration profile may be removed by a user without knowledge of the passcode, but this involves wiping the contents of the phone.) This feature allows a corporate IT department to select the security policies they deem necessary and roll these out across a fleet of iPhones relatively cheaply. In particular, the default user authentication policies may be strengthened using configuration profiles.

Even with a strong password policy enforced, there are loopholes available that allow this to be bypassed. For example, the digital assistant built into the iPhone 4S, known as Siri, allows users to issue voice queries to the iPhone which consult the user's address book (among other data sources) without ever requiring the passcode to be entered [14]. An unauthorised user could exploit this by picking up the iPhone and asking it various questions that are designed to leak valuable information. It is possible to disable Siri entirely, either using the menus or as part of a corporate configuration profile [13], however this removes a key feature of the iPhone 4S that many users will expect. It is possible to disable just the use of Siri from a locked screen, however as at October 2011 this could only be achieved using menus that remain accessible to the user; the configuration was not available for use in configuration profiles (according to [14]). Moreover, Apple's October 2011 guide on the use of configuration profiles [13] lists a setting for enabling or disabling Siri but makes no mention of any setting for controlling the use of Siri from a locked phone specifically. The more recent iOS hardening guide from DSD [9], however, explicitly calls for configuration profiles to be used to disable Siri's accessibility from a locked phone (p. 12). It seems that this feature may have been added very recently, and if so it should definitely be configured in the way that DSD recommends, however as at May 2012 the author can still find no mention of the availability of this setting in any Apple literature. Until this feature is supported by configuration profiles, a corporate IT manager only has two options available: either disable Siri entirely as part of the corporate configuration profile that is installed on employees' phones prior to them being authorised for professional use, or accept the fact that employees may enable PIN independent access to Siri at any time.

2.3 Phone to Network Authentication

Authentication of the user to the phone is not the only authentication that is required. Additionally, it is necessary for the phone to authenticate itself to the network. That is, some mechanism must be in place to prevent an attacker from impersonating a legitimate user's phone, as otherwise the attacker could send text messages that appear to come from the legitimate user's number or simply use telecommunication services at the legitimate user's expense. Older GSM (2G) phones are authenticated to the network using a unique shared secret number (Ki) that is stored on the phone's SIM card and also at the authentication centre (which is part of the network switching subsystem run by the mobile phone operator). This shared secret is used in a challenge-response authentication procedure [15]. More specifically, the authentication centre sends the phone a random number, which is passed to the SIM card and there combined with Ki using a predefined mathematical function. The SIM card sends the resulting output number back to the authentication centre (via the phone), after which the authentication centre can verify the response by repeating the calculation (based on its own copy of Ki). As Ki is never transmitted, it remains a secret buried in the SIM card's memory chip and impersonation attacks are impossible without this information. Authentication of (3G) smartphones works in a similar manner, although the details of the algorithms and functions have changed [16].

There are also known vulnerabilities in the mechanisms used for authenticating mobile phones to the network. It is possible to extract the secret key from the SIM card of many GSM (2G) phones or to clone their SIM cards [17], which makes the illegal impersonation of another network user fairly simple if an attacker has physical access to a victim's phone for long enough to make the clone. The protection of the secret key, however, prevents it from being read easily, so such attacks must either use very sophisticated digital forensics hardware (e.g. to read electronic state information from inside the chip) or else infer the value of the secret key by giving it a large number of authentication challenges and recording the responses for analysis. The latter approach is feasible only for version 1 SIM cards that were issued prior to around 2002; newer versions of SIM cards are programmed to enter a locked state if a large number of authentication challenges are received in a short period of time [18]. Some people have claimed to have successfully cloned later types of SIM cards [19], however such claims are controversial and difficult to replicate [20].

Another obstacle that must be overcome in carrying out a successful impersonation attack is that the network operator can prevent two different phones from being simultaneously connected to the network on the same SIM, or raise an alarm if the same SIM is used in two geographically distant locations in close succession. Radio fingerprinting of the phone is also possible, although there are innocent reasons why the radio fingerprint associated with a given SIM card could change suddenly (such as a phone upgrade). Alternatively, the subscriber identity information from the SIM can be cross referenced to the phone's International Mobile Equipment Identity number, with an alarm raised if the subscriber's identity is used from an unexpected phone. However, as with radio fingerprinting, this approach may cause a false alarm if the legitimate user upgrades his / her phone. Moreover, there are ways of illegally modifying IMEI numbers [21] (with some technical difficulty [22]), and so an attacker could clone a victim's IMEI in order to avoid detection by this means.

2.4 Network to Phone Authentication

It is also important for the network to be authenticated to the phone. If this were not done, then an eavesdropper could trick the user's phone into communicating with a false mobile phone tower (known as an IMSI-catcher) rather than with the network provider. Whether or not network to phone authentication is done is dependent on the protocol in use, which may be GSM (2G) or UMTS (3G).

2.4.1 GSM

The lack of any mechanism for authenticating the GSM network to phones makes such attacks relatively easy on GSM phones [23]. However, a simple impersonation attack (i.e. involving no parties other than the victim and the attacker) is likely to be detected when the victim uses voice services, as the attacker cannot fake the remote half of a voice conversation convincingly. On the other hand, this style of attack could be used to send the victim a fake text message purporting to be from one of the victim's contacts, in the hope that it elicits a reply that yields valuable information.

A more useful attack involves forwarding traffic to and from the legitimate network provider, i.e. when the attacker is a man-in-the-middle who impersonates the legitimate network to the user's phone and impersonates the legitimate user's phone to the network. The authentication challenges issued by the network can be dealt with by verbatim forwarding of the challenges and responses between the legitimate parties. This style of attack is usually of limited utility, since the data subsequently transferred is encrypted using a key derived from a shared secret known only to the network provider and the user's SIM card. As the man-in-the-middle has no knowledge of the encryption key, the use of encryption prevents him / her from reading the data being forwarded in each direction and from making meaningful modifications to it.

Unfortunately, the GSM protocol does not protect the integrity of all the messages used to negotiate the choice of encryption algorithm [23]. Hence, a man-in-the-middle can eavesdrop by modifying these messages, to request the use of very weak encryption or none at all. As far as the author is aware, this vulnerability still exists.

2.4.2 UMTS

As smartphones typically use the newer UMTS (3G) standard rather than GSM (2G), the vulnerability in GSM is not usually an issue for them. However, many smartphones will revert to using GSM when no UMTS service is available and therefore could be vulnerable. (This is a situation that could occur in remote locations or may be engineered by an attacker with the ability to block UMTS services in vicinity of the victim.) On some smartphones, the use of a GSM connection with weak encryption would result in a warning being displayed to the user, however doing so is an optional part of the UMTS standard [23] and so this may not occur on all smartphones. Even if a warning is provided, some users may not appreciate its significance and may be unaware that their communications may be compromised.

The UMTS standard includes authentication of the network, which makes impersonation of a 3G network much more difficult [24]. The UMTS standard also protects against more subtle attacks, such as a man-in-the-middle replaying valid authentication credentials between the two parties but with modifications to the security mode command message that disable the use of encryption (essentially the same attack as described above for GSM). This is because the security mode command message includes a digitally signed message authentication code, that can be used to check the integrity of the message [23]. For this reason, smartphone security may be significantly improved if they are configured never to use GSM connections, or at least never to use GSM connections with weak encryption.

2.5 Data Transmission Confidentiality

When a smartphone is communicating with the network, it is crucial for the signal to be encrypted in order to maintain confidentiality of the data being transmitted, i.e. prevent eavesdropping. With UMTS (3G) phones, this is done using the f8 confidentiality algorithm, which depends on a shared secret 128 bit key CK [25, 26]. The author is not aware of any vulnerability in this encryption scheme. As with any encrypted data transmitted through a publicly accessible medium, there is always a risk that adversaries may intercept and store encrypted UMTS traffic for future cryptographic analysis. However, doing so would be computationally expensive and may not yield results for a long time, limiting the usefulness of such an attack. This is especially true for adversaries without the ability to predict which intercepts are likely to contain valuable information, as this lack would prevent them from concentrating their efforts where it matters.

2.6 Data Transmission Integrity

Another important issue is the ability to detect any modifications that an attacker makes to the data whilst in transit between the phone and basestation, or vice versa. With UMTS (3G) phones, this is done using the f9 integrity algorithm, which depends on a shared secret 128 bit key IK [25]. Note that IK and CK have different values. The author is not aware of any vulnerability in this integrity verification scheme.

2.7 Confidentiality, Integrity and Authentication using Other Protocols

At this point, it should be noted that the security issues relating to mutual authentication of the smartphone and the network, as well as those relating to the confidentiality and integrity of the data, are also pertinent to other types of communication that are available on many smartphones. For example, some phones include WiFi, Bluetooth or NFC capabilities. Such capabilities provide the user with more flexibility and a wider range of functionality, however they also increase the security risk, since each communication system that is supported represents a potential line of attack. For the sake of brevity, an outline of how security issues are addressed in these protocols is not provided here, although some of their known vulnerabilities are discussed.

2.7.1 NFC

NFC, for example, offers possibilities for attacks [27], although the limited amount of operational experience of NFC enabled smartphones means it is difficult to predict the range of vulnerabilities that may exist. The biggest issue with NFC was that the original standards defining it [28, 29] did not include any security specifications for authentication or for ensuring the confidentiality or integrity of transmitted data. Hence, security functions were to be provided by the services that use NFC, which are application specific. More recently, additional standards have been published [30, 31] (there are also free versions available at [32, 33]) which specify the implementation of a security layer between the underlying NFC service and specific applications, commonly referred to as NFC-SEC. The NFC-SEC standard covers the use of cryptographic techniques for ensuring confidentiality and integrity, however it does not specify any means for authenticating the parties involved in an NFC transaction as there is no pre-existing shared secret which can be used for this purpose ([34], p. 16). In principle, this leaves the protocol vulnerable to man-in-the-middle attacks. However, the technical difficulties of carrying out such an attack without detection are extreme, since both legitimate parties can listen whilst transmitting to determine if another NFC device is attempting to override the signal being sent [35].

There are a number of possible types of attack which this argument fails to address, however. One is a range extension attack, where a rogue NFC device is hidden within range of a legitimate NFC device, for example a device that deducts a fare from a public transport customer’s account. If a customer’s mobile device comes within range of the rogue NFC service before coming within range of the legitimate service, then there is no need for the attacker to override the signals sent by either legitimate party. (Some kind of directional transmission may be needed in order to avoid each legitimate party detecting the attacker’s transmission to the other legitimate party.) Since the user is expecting a transaction at about that time, the user may agree to authorise any transaction proposed by the attacker. Moreover, when the legitimate parties later come within range of each other, they will both believe that a valid transaction has already taken place and will ignore each other, just as they would in the case where a legitimate transaction had actually taken place and then the devices had come within range a second time.

Another possible attack is an isolated rogue transmitter hidden in a location where the user does not expect any NFC transactions (e.g. a park bench), although that would require pre-existing malware on the victim’s phone for the device to communicate with [27]. One solution to the vulnerabilities remaining in NFC would be to develop a public key infrastructure for NFC, based on digital certificates whose authenticity can be verified using a master public key that is either included in mobile phone operating systems or else included with the application that the user installed to access the service. Unless such measures are in place, NFC services should be treated with caution.

2.7.2 Bluetooth

While a more mature technology, Bluetooth has several known vulnerabilities [36], especially if configured incorrectly (e.g. enabling "just works" [36] pairing of devices). Some of Bluetooth's security protocols are extremely poorly designed, such as sharing the master key on-air [36]. For these reasons, among others, it is generally recommended to disable Bluetooth on devices carrying sensitive information [37] and to choose Bluetooth settings carefully on other devices [38].

2.7.3 WiFi

WiFi is more mature than NFC and can be made reasonably secure, providing that the WiFi network is configured correctly, e.g. to use the WPA2 security protocol rather than the earlier WPA or WEP protocols [39]. More recently, however, it has become apparent that many WiFi routers are vulnerable [40] to brute force attacks on the PIN used in the WPS standard (which is an addition to WPA2 that is intended to make the setup of secure wireless connections easier for the user). This type of attack can allow unauthorised users access to private WiFi networks, which means a WiFi network that is believed to be private may not be in practice. Some types of router are able to be configured to turn off WPS, thus avoiding this issue. In any case the security of WiFi varies from network to network, and an unknown or public network should always be treated with caution.

2.8 Security Policy Consistency

When a smartphone is in use while its user is travelling, the smartphone may need to roam across a variety of different networks in order to maintain connectivity. In some cases, the areas covered by different network providers may vary, with the users of one network provider using the basestations belonging to another under reciprocal agreements, in order to maximise the coverage available. In such cases there may be differences in the implementation details of the protocols used, which can affect the quality of service and could result in inconsistencies in the security policies applied. In particular, it is very difficult to guarantee security during the handover procedure itself, since in this case the protocol that is followed may be a complex and poorly defined mixture of the protocols used by the two different network providers. Even more complex security and quality of service concerns can arise if the handover involves a change to a completely different type of protocol, e.g. changing from a 3G to a 2G network. These issues are acknowledged in [41].

There are ongoing research efforts [42] to develop a standard for a protocol called Media Independent Handover, which aims to make network-to-network and protocol-to-protocol handover operations seamless. Unfortunately, most of the necessary security features are not yet part of this standard; however, some brief descriptions of expected security issues are provided in [42]. These include the potential for an attacker to impersonate a mobility server on the host network, the possibility that an attacker could modify the network information sent from a mobility server to the smartphone without detection, the ability for attackers to record messages from mobility servers and replay them later (or elsewhere) in order to cause the smartphone to attempt an invalid handover, and the likelihood that attackers could eavesdrop on communications between the mobility servers and the smartphone in order to trace the movements of a user. This raises privacy issues similar to those discussed in Section 2.12.

2.9 Side-Channels

There is a long history of research on unintentional electromagnetic emissions from electronic equipment. This covers the means by which electromagnetic emissions may be exploited to reveal information being processed on equipment operated by adversaries, as well as methods that may be used to increase the difficulty of such attacks on equipment operated by friendly forces. Research on such topics goes back to the NSA's TEMPEST programme, from which many documents have been released into the public domain (with many redactions) following freedom-of-information requests [43]. Obviously, the early work on this topic does not relate to smartphones, however many of the principles involved with analysing stray electromagnetic signals are still relevant.

More recently, successful side-channel attacks on smartphones have been demonstrated, based on eavesdropping on stray electromagnetic radiation from smartphones' internal circuitry. Specifically, it is possible to read the RSA private key used in an Android application on a HTC Evo 4G, using a loop of wire held in close proximity to it. A close range attack was also demonstrated on another HTC device doing AES encryption, as well as a longer range (10 feet) attack on an iPod Touch running an application that performs elliptic curve cryptography [44, 45]. Alternative side-channel attacks based on an analysis of power consumption are also discussed in [45], although this approach is more invasive. The problem is that all cryptographic computations must be performed on some hardware, and this requires the cryptographic key material to be loaded into memory and / or CPU registers prior to its use. The transmission of the data through various buses and its subsequent processing in the CPU create electromagnetic emission as a side effect [46], and it is sometimes possible to detect such emissions and determine what the original data must have been. In addition, the processing of the data has a measurable effect on the power consumption of the CPU, so that the time variation in the power drawn can be used to infer the bits making up the data. If cryptographic key material is able to be read in this manner by an unauthorised device near a smartphone, then many of the security functions of the phone may be rendered vulnerable. For example, reading the key used to block-encrypt the data stored on the device would allow an attacker who later took possession of the smartphone to read the phone's contents in plaintext. If other keys could be read, then a variety of other attacks could be facilitated.

There is another known side-channel, which arises because the time taken to perform cryptographic computations can vary in a way that may be correlated with the value of the secret key. The details of how this may be achieved will not be discussed here, however the curious reader is referred to [47] for a full explanation. Traditionally, such timing attacks were only considered a possibility when the attacker has physical access to the hardware that performs the cryptographic computations, such as a stolen smartcard. More recently, remote timing attacks have been demonstrated [48], despite the unpredictable delays that remoteness introduces. (The attack described in [48] can also be considered a type of fault injection attack, since malformed but specially chosen messages involved in the key exchange protocol are used to ensure that the timing yields useful information about the private key.) The precise conditions under which an adversary could successfully perform such an attack on a smartphone are difficult to predict and there are several potential smartphone functions that may be vulnerable. For example, some phones allow a remote login as a security feature for activating the camera, GPS or remote wipe on a stolen phone; a remote adversary could use a timing attack against the user authentication for this feature, since the time taken to reject various passwords of the attacker's devising could leak important information about the real password. Alternatively, an eavesdropper on the authentication exchanges between a phone and a basestation could use the delay times of the responses to the authentication challenges to reduce the number of challenge-response pairs required to derive the shared secret.

An adversary with physical access to a device performing cryptographic computations can also manipulate its operating environment to induce errors in the computation, potentially causing useful information to be revealed in the process. This is the classic form of the fault injection attack, as described in [49]. Typically, the attack involves modifying the power supply voltage to the processor, so that is outside of the normal operational range, either for an extended period of time or as a short spike [49]. Other environmental manipulations are also possible, such as a running the processor in an abnormal ambient temperature [50] or with an impaired cooling system. It has been shown that the introduction of errors into public key cryptographic computations can result in output, which although incorrect, may be used by the attacker to compute the private key (with minimal computational expense) [49]. There is a possibility that some cryptographic functions on a stolen smartphone could be compromised in this way.

In the case where a smartphone is running several enclaves at different security levels on the same hardware, with certified software to prevent data leakage between the domains, there is also the risk of cache attacks. In this attack, the untrusted software running in one security domain may infer useful information about the memory used by another enclave by the time it takes to fulfil memory read requests. For example, a rogue process may deliberately fill the cache by reading from a selection of memory locations in its own address space. Subsequent read operations from these locations will be served very quickly as the necessary data will be in the cache, unless some other process (possibly running in a different enclave) has replaced some of the cache entries through its own memory use. By timing the speed of the read operations, the rogue process may be able to detect when another processes is accessing memory and important clues about the pattern of usage [51]. The potential for cache based side channels is one of the many things that must be eliminated when designing hypervisors and carefully considered prior to certifying them. The certification for the Green Hills Platform for Trusted Mobile Devices (see Section 4.2.4), for example, considers side channels using the level one cache but does not consider side channels using the level two cache ([52], p. 13), and so the level two cache must be disabled.

2.10 Application Level Vulnerabilities

Even if a smartphone has no security vulnerabilities in its hardware or operating system, vulnerabilities may be introduced by the installation of applications that deliberately or inadvertently compromise the device. The extent to which this is an issue depends on the operating system. On (non-jailbroken) devices with iOS, for example, the applications that are available for installation are tightly controlled by Apple, with malware detection a critical part of the screening process [53]. While this reduces the threat considerably, there are no guarantees that the vetting process will detect all attempts to hide malware in an otherwise normal application. For example, an iOS application was developed recently that was distributed through Apple's application store, but acted as an agent for downloading and installing malware from a remote server [54]. While the author, Charlie Miller, is a 'white hat' hacker whose aim was to draw attention to oversights in Apple's application vetting process, it is possible that 'black hat' hackers could attempt similar attacks in future. Moreover, legitimate applications could contain bugs that are subtle enough to escape the notice of Apple's vetting team but which an attacker is able to exploit; in fact, Miller's malware application exploited a security loophole introduced by Apple's Safari browser [55]. Of course, if a particular application is known to cause problems Apple can remove it, however that would be too late for users who have already been affected.

Apple's use of configuration profiles [13] can help to limit the damage from malware or genuine software containing bugs that the attacker has exploited. This is because security settings that are specified by an active configuration profile cannot be modified by an application in order to facilitate its attack. On the other hand, an application can install its own configuration profiles (only with user permission), and security settings not configured by an existing profile may be weakened by this.

The malware risk is increased significantly if an iPhone is jailbroken. This is mainly because jailbreaking allows applications to be installed from a range of third parties whose products are not vetted by Apple. While the device's functionality may be expanded by doing so, the extra applications that this allows are not always what they claim to be. A number of viruses are known to infect only jailbroken iPhones, such as the Duh virus and its predecessor Ikee [56]. By jailbreaking an iPhone, the user must accept responsibility for the device's application level security, rather than relying on Apple to do this.

In contrast, off-the-shelf smartphones using the Android operating system can install applications from GooglePlay (formerly Android Market) that have not been vetted [57], as well as applications from other sources. While Google can remove applications from GooglePlay that are known to contain malware, many users may be affected before this happens. Moreover, Google has no ability to remove malware applications that are distributed via third parties. As an open source operating system, Android is particularly attractive for malware authors looking for vulnerabilities. Android malware has grown rapidly in recent times, surging 472% between July and November 2011 [58]. There is also a risk of vulnerabilities in genuine applications created by careless or uninformed developers, that hackers may learn to exploit [59]. (This is an issue with other smartphone operating systems also, although in the case of iOS there is at least a chance that the vetting process will uncover such bugs.)

In order to limit the damage that third party applications can do, both Android and the iPhone run each application in a 'sandbox' [60, 61], which prevents the application from accessing data and system resources unless the user provides the necessary permissions at installation. However, whether the permissions that are available on Android are comprehensive enough and provide sufficiently fine granularity is a matter of debate [62] and users may be unaware of the full implications of granting a particular permission. Third party applications do exist which allow finer permissions to be granted, for example using Mr Hide to mediate access to all system privileges and using Dr Android to transform other applications so that they obtain very fine-grained permissions from Mr Hide rather than directly from the system [63].

Moreover, a cleverly designed malware application can trick the user into granting the permissions it needs by mimicking an existing, legitimate application that requires the same permissions. For example, malware has appeared on Android smartphones, disguised as the Trusteer Rapport banking security tool, which intercepts SMS messages and forwards them to a remote server [64, 65]. There is speculation that this particular piece of malware is associated with Zeus [66], and is intended to capture the one-time tokens that some banks use as a second authentication factor. This malware is distributed from a rogue webserver rather than through GooglePlay [64], although it is not clear from the available literature what the nature of the attack vector is (e.g. pop-up, link in spam email, user initiated installation, exploit of vulnerability in port listening service, etc).

2.11 Confidentiality in the User's Physical Environment

If smartphones are used by an authorised user in a public place, there still is a serious risk that information could be leaked to persons for whom it was not intended. This could be the result of unauthorised persons 'shoulder surfing' to view the contents of the smartphone's screen or listening in on conversations or audio playback. Moreover, many physical environments include CCTV security cameras that could be used to capture screenshots containing sensitive information. There is also a chance of covert cameras or listening devices being placed in the user's physical environment for commercial or foreign espionage purposes, especially in hotel rooms that are frequently used to accommodate conference attendees. This issue would be of particular concern if users were able to access national security classified information from smartphones.

Note that the physical environment can also facilitate attacks relating to other issues discussed previously. For example, an analysis of the grime on the phone's keypad could provide useful information concerning the characters that are likely to appear in the user's login password, especially if the user unlocks the phone frequently but changes the password rarely. Electromagnetic radiation from the phone's internal circuitry could yield useful information about the data being processed in unencrypted form (see Section 2.9). Finally, physical access to the phone's SIM card is essential if the SIM is to be duplicated as part of an impersonation attack, or if some kind of electronic bugging device is to be inserted into the phone.

Note that many of the attacks that are possible in the physical domain could be carried out more effectively in the software domain, e.g. if the user unwittingly installs a keylogger or some other malicious application on the phone. This was discussed in more detail in Section 2.10.

2.12 Privacy Issues

Many commercial smartphones include software that collects usage metrics from individual phones, with the aggregated statistics provided to network operators for monitoring and improving quality of service. While there are some merits to such activities, questions have been asked about the scope of the data that is collected and the extent to which its collection may violate users' privacy. CarrierIQ is an example of such software, which is commonly deployed on Android and Blackberry smartphones [67]. This software is capable of capturing a very wide range of usage data, including user keystrokes, the device's geographical location and installed applications [68]. The capturing of such data and subsequent transmission to various third parties is not acceptable on a device used to handle sensitive government information, and therefore must be disabled.

3. Additional Issues in the Corporate Context

This section considers some extra issues (i.e. in addition to those in Section 2) that arise for smartphone usage in a corporate context. There are two broad paradigms for the use of smartphones within organisations: the traditional model where the devices are provided by the organisation for mainly professional use, and the bring-your-own-device model where employees purchase their own devices for mixed personal and professional use. The issues that arise under these paradigms are the subjects of Section 3.1 and Section 3.2 respectively. There are yet more issues to consider in the case where the corporate context in question is a government agency, which are discussed in Section 3.3.

3.1 Additional Issues Under the Traditional Corporate Information Technology Paradigm

This section considers some extra issues that arise when a smartphone is used under the traditional corporate information technology paradigm, that is, when the device is selected, supplied, owned and administered by the organisation, primarily for professional use. It is assumed that the network service provider is also selected by the organisation and that the billing is to the organisation.

3.1.1 Information Separation and Ownership

It is desirable for personal and business information stored on the device to be kept as separate as possible. If effective separation is possible with the chosen technology, then this allows different policies to be applied to the personal and professional data. If not, it may be very difficult to develop a set of policies for appropriate handling of the mixed data stored on the device. Moreover, there may be privacy issues relating to personal information being exposed to corporate information technology administrators, and legal liabilities if this information is inadvertently leaked by the organisation. The organisation may also bear some responsibility for the integrity of the user's personal data, if the user relies on it as their only copy (e.g. the user's personal address book). The extent to which this is the case will vary, depending on the terms and conditions of use to which the employee agreed before being issued with the device.

In this paradigm, the organisation owns the device and much of the information stored on it; however any personal information stored on the phone belongs to the employee. This could result in conflicts in certain situations, such as when the device is disposed of at the end of its lifetime, or when the device is returned to the organisation upon cessation of employment. In the case of disposal, the interest of the organisation is best served by wiping all data from the device. The employee, on the other hand, may expect the opportunity to copy personal data off the phone before this takes place, an act which has the potential to leak valuable corporate data. In the case of returning the phone to the organisation, the organisation may choose to wipe the data or simply re-purpose the device for use by another employee; if the latter, then the phone's original user may have valid privacy concerns that are not fully addressed by the user's attempts to move personal data off the device manually. Clearly, such issues would be easier to resolve if the technology were to provide reliable separation of professional and personal data.

The need to separate personal and professional information is related to the problem of handling multiple levels of security for sensitive government information, about which much has been written elsewhere [69]. A smartphone separating personal and professional information could be considered a two level MLS device.

3.1.2 Loss of Authorised Custody of the Smartphone

In the event of an organisation's smartphone being lost or stolen, or perhaps being illegally retained by the employee using it upon leaving the organisation, the risk of corporate data being leaked is heightened. Hence, it is necessary for the organisation to develop policies for dealing with such situations which aim to minimise the damage that results. Many smartphones have features that can assist in these situations, such as the ability to wipe the contents of a smartphone remotely or trace a lost phone to a certain area. If the smartphone in question has such capabilities, then the organisation's interests can best be served by attempting to wipe all sensitive information remotely as soon as the incident is reported and then trying to do a trace, with any information obtained being handed over to the police if necessary.

There are dangers to this approach, however, especially in the case of a lost phone. If the remote wipe function is activated without the employee's permission and the smartphone includes personal data that is finely mixed with professional data, then the organisation could be held responsible for the loss of personal data (albeit only if the phone is subsequently recovered). This is another case where strict separation of the personal and professional data would help, as then the remote wipe instigated by the organisation could wipe the corporate data only, with the employee free to decide whether or not to carry out a remote wipe of the personal data.

Attempting to trace a phone which was or is in the custody of an employee or ex-employee also runs the risk of violating that person's privacy. For example, situations could arise where the phone is traced to a location that compromises the employee's reputation. The legal implications of such potential outcomes need be taken into account when formulating a policy relating to the use of phone tracing.

3.1.3 Sharing Administration Rights with the User

Under the traditional corporate information technology paradigm, the organisation has administration rights on the device since it is owned by the organisation. In some cases, the employee using the device may be granted administration rights also, perhaps with some limitations.

In the case of smartphones, the ability to download and install a wide variety of applications for various purposes is fundamental to the experience of using it and essential for obtaining the utility that users expect. If employees are not granted administration rights to their smartphones, therefore, they may resent the inability to install particular applications that they want or the inconvenience of having to get this done through slow and cumbersome corporate systems. In addition, employees who are forced rely on the organisation's IT department for making administrative changes to the smartphone will be unable to obtain a timely fix for problems that arise after business hours, even if they have the technical skills to fix such problems for themselves. On the other hand, granting employees administration rights would allow them to install applications that may contain malware or to modify settings in a way that could compromise the organisation's security. It is possible to maintain security and allow some user flexibility if the smartphone has separated enclaves for personal and professional use, so that the employee can be granted administration rights only in the personal enclave, without the security of the professional enclave being affected.

3.1.4 Personnel and Safety Issues

Since the employee is provided with a specific phone to use under the traditional paradigm, the organisation's choice of device and / or network service provider may not be to every employee's taste. In particular, employees who have developed brand loyalty to a particular type of smartphone may be annoyed at being forced to use another kind at work. This could result in dissatisfaction and poor user performance when navigating the device's interface. In the worst case, the user may attempt to use a personal device for work in place of the official device. (While this would be contrary to policy, it may be difficult to police in some cases.) Even if the employee has no particular preferences regarding smartphone types, the difficulties associated with carrying two smartphones may encourage the employee to switch his/her professional usage to his/her personal device or vice versa.

Another issue to consider is the extent to which smartphones allow an employee's job to encroach on his / her personal life, sometimes known as "time pollution" [70]. While this problem has existed to some degree since landline telephones first became common in private dwellings, the introduction of mobile communications has worsened the situation by making employees contactable at any time. The introduction of smartphones means that employees are now also contactable by email at any time, and always have the facilities for performing complex processing tasks (e.g. manipulating data in a spreadsheet) when preparing a response. While such flexibility can be useful for dealing with urgent operational matters, it can increase employee's stress levels if it occurs too often or there is an expectation that employees should respond promptly to such interruptions. In the longer term, the associated damage to morale and wellbeing could have a detrimental effect on productivity [70]. Some organisations deal with this by limiting the times during which employees can be contacted for queries relating to work [70], however the effectiveness of such policies is limited by the fact that many queries may come from outside the organisation, e.g. from customers or suppliers.

The developing workplace culture that has accompanied the introduction of smartphones could also cause health and safety issues in extreme cases. For example, the expectation of responding promptly may encourage some employees to answer calls or texts when driving. Alternatively, interruptions from a mobile phone when an employee is at work could cause the employee to make a mistake which puts the health and safety of others at risk, e.g. when operating machinery.

3.1.5 Financial Issues

Some employees may take advantage of a smartphone provided by their employer through excessive personal use of the phone. While a minor level of personal use at the expense of the organisation may be tolerated, there are limits to the amount of free usage that employers can be expected to pay for. An organisation could develop guidelines for what constitutes fair and reasonable personal use, however these may be difficult to define in precise terms and even harder to enforce. The organisation always has the option of putting a cap on the total cost that the organisation pays for each smartphone every month, with additional usage either disallowed under the terms of the plan or charged to the employee, however that may be unfair to the employee if operational requirements in a particular month demand an unusually high level of usage. Fairness could best be achieved if it were possible to track personal and professional usage separately, and reallocate the bills accordingly.

3.2 Additional Issues Under the Bring-Your-Own-Device Paradigm

This section considers some extra issues that arise (i.e. in addition to those in Section 2) when a smartphone is used under the bring-your-own-device paradigm, that is when the device is selected, supplied, owned and administered by the employee, primarily for personal use. It is assumed that the network service provider is also selected by the employee and that the billing is to the employee. The bring-your-own-device paradigm could apply when an organisation does not supply employees with phones at all, or when an employee chooses to use a personal phone instead of one supplied by the organisation.

3.2.1 Information separation and ownership

It is desirable to keep personal and business information separate under the bring-your-own-device paradigm, as it is under the traditional corporate information technology paradigm discussed in Section 3.1. In this case, there may be security and / or commercial risks relating to professional information being inadvertently disclosed to the employee's personal contacts. The employee may also bear some responsibility for the integrity of any professional data stored on the phone, if this is the organisation's only copy (e.g. if the employee is working on a document that is stored locally on a smartphone), and inadequate separation may make the creation of backups or synchronisation with copies on the corporate network more difficult.

In this paradigm, the employee owns the device and much of the information stored on it, however any professional information stored on the phone belongs to the organisation. This could result in conflicts in certain situations, such as when the device is disposed of at the end of its lifetime or when the employee leaves the organisation. In either case, the organisation may wish to remove all the professional information from the smartphone, in order to protect the confidentiality of its data. If the distinction between professional and personal data is not clear, then the only reliable way to do this may be to wipe all data from the smartphone. However, since the device storing the information is owned by the employee, it is questionable if the organisation has the legal right to wipe data from the phone [71].

In the specific case of device disposal, there is nothing for the employee to lose by letting the organisation wipe all data off the device, providing that first the employee has the opportunity of copying personal information onto a new device. However, if the separation of personal and professional data is not clear, then such a copy operation carries a strong risk of the inadvertent inclusion of the organisation's sensitive data, and hence the risk of subsequent leakage. The employee and organisation may therefore disagree on whether or not employees should be allowed to copy personal data off smartphones prior to their sanitisation.

In the specific case of an employee leaving the organisation, it is unlikely that the employee would be willing to have his / her smartphone sanitised if this meant losing personal data (with or without the opportunity to make a backup) or having to reinstall software. In either case, even if the employee had signed a waiver agreeing to allow all data on the phone to be destroyed upon disposing of the device or leaving the organisation's employ, it would be very difficult to prevent the employee making an unauthorised backup of the data on his / her own phone.

3.2.2 Loss of Custody of the Smartphone

The issues to consider when developing a policy to handle lost or stolen smartphones were discussed in Section 3.1.2, as regards smartphones owned by the organisation. The same issues apply to phones owned by employees, except that the phone cannot be illegally retained by an employee in this case. It should also be noted that, when the phone is owned by the employee, the organisation's legal position may be weakened in terms of what it is allowed to do to a phone that it does not own [71].

In some cases, the interests of the organisation and employee may be aligned. For example, remote wiping a stolen phone is in the interest of both the employee and the organisation, as long as both parties are concerned about disclosure of their confidential information. On the other hand, conflicts may arise when a phone is lost but the employee believes that its recovery is likely. In that case, the employee may want to delay wiping the phone's data until all possibility of recovery has been exhausted, while the organisation may wish to wipe the phone as soon as possible in order to limit the risk of data leakage. Obviously, such conflicts are trivial to resolve if the personal and professional data are kept separate, as then both parties may follow their own policies regarding remote wiping of their own data.

3.2.3 Sharing Administration Rights with the Organisation

By default, administration rights on a phone owned an employee will be held by the employee, and only by the employee. This state of affairs, however, may place the organisation's sensitive data at risk, as the employee may not have the necessary maintenance skills required for keeping the operating system secure. If the employee is willing to grant administration privileges to the organisation then this would no longer be an issue, as the IT staff would be able to take care of such matters on behalf of the employee. (Of course, this would also introduce new issues, such as the need to maintain the confidentiality and integrity of the personal data on the phone that the IT staff would then have access to.) If the employee is not willing to grant administration privileges to the organisation when asked, then the organisation could do nothing other than banning the employee from using the device for processing the organisation's information, and even this would be very difficult to enforce.

Even if the employee does grant administration privileges to the organisation, there are still significant security risks remaining due to the employee retaining administration rights. When acting as an administrator, the employee could install applications containing malware, modify operating system settings that are critical for security, or disable security software such as virus checkers and firewalls. This could be resolved by requiring employees to relinquish administration rights before a personal phone is allowed to handle the organisation's data. Many employees may be unwilling to accept such conditions, however, as the ability to install a wide variety of applications is a fundamental part of the functionality that users expect from smartphones.

3.2.4 Personnel and Safety Issues

It is possible that the bring-your-own-device paradigm will become the cultural norm in most workplaces, sometime in the near future. In many workplaces, this is already the case [71]. One of the possible negative side effects of this is that employees who are not willing or able to provide a phone may be discriminated against by employers. There is precedent for this type of discrimination, for example delivery drivers who are expected to provide their own cars or trade practitioners who are expected to have their own tools. The addition of the smartphone as a necessary tool for certain jobs would increase the barriers to employment for the underprivileged.

The issues of "time pollution" and safety also apply to employee owned smartphones, just as they do to employer owned smartphones (see Section 3.1.4).

3.2.5 Financial Issues

The question arises as to whether it is fair to expect employees to pay for professional usage of their phones. While a minor level of professional use at the expense of the employee may be tolerated by some people, there are limits to the amount of usage that employees can be expected to pay for. In many cases, users who would not normally be happy to pay for their professional usage may choose to do so because of the convenience of using a personal smartphone, especially in the case where no mobile communication device is supplied by the organisation. There is a risk that organisations will exploit this convenience factor to extract maximum benefit from phones that are billed to employees.

Of course, Australian employees can recoup some of the expense of professional phone use through claiming a tax deduction from their income. However, it may be difficult to obtain an accurate estimate of the breakdown between personal and professional usage. Moreover, employees are still left financially worse off from paying for professional phone usage then getting a tax deduction for it, than if the employer had paid.

Fairness could best be achieved if it were possible to track personal and professional usage separately, so that the organisation can reimburse users for the professional usage expense. Even if no reimbursement policy were in place, this information would be helpful for allowing employees to make an accurate tax deduction.

3.3 Issues Specific to the Australian Government Context

This section considers some extra issues that arise in an Australian Government context. These issues are additional to the issues raised in Section 2, as well as those raised in Section 3.1 or Section 3.2, depending on the usage paradigm.

The primary difference between government and non-government organisations (in this context) is that governments handle information on behalf of all their citizens, whereas most non-government organisations only handle information that they own themselves or which they hold on behalf of a limited number of customers. While both have a duty of care to protect the confidentiality of data that is owned by other parties, the unauthorised disclosure of sensitive government data has the potential for more severe and widespread consequences. In addition, Australia's intelligence sharing agreements with various allies means that unauthorised disclosure of information in Australian Government custody could have an even wider impact. If smartphones are to be used within Australian Government, therefore, it is even more critical that the security issues raised are taken seriously, especially those relating to confidentiality. When handling sensitive information belonging to an ally, it is also important that the ally's security policies regarding smartphones are taken into account when determining how (or if) smartphones may be involved.

As a result of the above considerations, new information and communication technologies need to go through a formal certification process before they can be authorised to handle sensitive government data. The certification process is expensive and time consuming, which means that there can be a significant delay between when new technology becomes available for commercial use and when (or if) it becomes available for government use. In many cases, technology is already obsolete by the time it is certified [72] and may be near the end of its vendor-supported lifetime. This issue is particularly pressing for smartphones, since they are currently one of the more active areas for IT research and development.

One issue that is unique to government organisations is the need for handling information at multiple classifications. While private organisations may handle quite different types of sensitive information, e.g. customer accounts and intellectual property, it is unusual for them to have a formal classification system that is supported by separate network infrastructure at each classification level. In many corporate environments, it would be sufficient for data on smartphones to be segregated into just two divisions, namely the employee's personal data and the corporation's data. In many government organisations, however, it would be necessary to segregate the organisation's data on a smartphone into two or more different classifications, as well as keeping all these separate from the employee's personal data. For this reason, many smartphone segregation technologies aimed at the commercial market are inadequate for the needs of government organisations, since only two separated domains are provided. This is discussed further in Sections 4.2 and 4.3, which include reviews of some technologies that provide separated domains.

4. Smartphone Technology Review

4.1 Emerging Security Technology

4.1.1 Security Enhancing Software

A range of third party products exist for improving security on smartphones, especially phones running the Android operating system. These include Lookout (malware detection, cloud data backup service, GPS based lost phone tracking), Norton Mobile Security (malware detection, call and SMS blocking, remote locking or wiping of lost phone, remote locking of SIM card), McAfee's WaveSecure Mobile Security (remote locking or wiping of lost phone, data backup service), AVG Antivirus (malware detection), NetQin Anti-virus (malware detection, lost phone tracking, remote locking or wiping of lost phone, remotely activated alarm) [73], and McAfee Mobile Security and McAfee Family Protection Android Edition (malware detection, secured web browsing, location tracking, data backup service, remote device access, remote wipe) [74].

A number of applications are available for enhancing security on iOS devices, such as the iPhone. These include McAfee's WaveSecure Mobile Security (remote locking of lost phone, data backup service), Intego's VirusBarrier (malware detection in downloaded content only), Lookout Mobile Security (data backup services, lost phone tracking, remote wiping, and security warnings relating to operating system updates, jailbreaks and unsecured networks), GadgetTrak (remote activation of lost phone's camera and phone tracking), Firewall iP (firewall for jailbroken iPhones only), iLocalis (allows wide range of remote control functions on jailbroken iPhone), Webroot SecureWeb (browser), Junos Pulse (secure VPN connections to corporate networks) and Cisco AnyConnect (authentication services) [75].

A variety of security software products exist from other vendors and for other smartphone platforms, providing similar functionality to the products mentioned above. The lists in this section are not intended to be comprehensive, but merely to provide an indication of the range of products and services available.

4.1.2 User Authentication Technology

A recent development in user authentication technology on smartphones is the face recognition unlock for Android 4.0 – Ice Cream Sandwich [76]. This uses the phone's camera to take photos of the person holding a locked phone, and only unlocks the phone if it detects a face that matches that of the user it was trained to recognise. Within about a month or so of the technology's launch, however, a demonstration video emerged showing an Android phone being unlocked by holding an image of the expected face (displayed on another phone's screen) up to the camera [77]. Google claims that this is impossible (without providing any supporting evidence) [78] however as far as the author knows there have not yet been any independent demonstrations to confirm or deny this attack's efficacy. Nevertheless, there are reasons to be concerned about relying on facial recognition as a single factor of authentication.

The facial recognition technology could be improved to require a consistent stream of photos to be taken from a range of different points of view (hence preventing flat images from being accepted), using a randomly generated sequence of scanning motions which the user is asked to fulfil. Google have recently attempted something along vaguely similar lines to this, by requiring the user to blink during facial recognition [79]. However, it has been reported that it is possible to defeat this security measure also [80]. This may be achieved by editing a photo of the phone's owner so that the eyes are covered by a patch of skin cloned from elsewhere on the face, then holding the phone's camera up to the screen of a device displaying an alternating sequence of the modified and original photos.

Even if facial recognition could reliably discriminate between a genuine face and flat images, it still may not be secure: there are questions that may be asked about the statistical properties of the facial recognition analysis. For example, it would be instructive to find the probability that two randomly selected individuals look similar enough to match, as far as the facial recognition function is concerned. Ideally, an individual needs to know how many people from the population are similar enough to match his / her own face, although this is clearly impractical to determine. Moreover, if a smartphone with facial recognition unlocking is stolen along with some form of photographic identification, then it may be possible to fool it using face putty, false beards, etc to impersonate the owner.

An alternative user authentication method based on biometrics is to use a fingerprint scanner. This has been used as an alternative to a PIN on smartphones, for example on the Motorola Atrix 4G [81]. However, it has been shown that fingerprints left on glass surfaces may be scanned and used to create a mould for the production of a fake "gummy finger", which can fool typical commercial fingerprint scanners with a success rate of at least 67% [82]. This success rate is high enough to be of concern even with smartphones that lock down after a small number of failed authentication attempts (if that were the only authentication needed to unlock the phone). Moreover, the technique used to create the "gummy finger" is relatively simple and inexpensive, so that it is well within the capabilities of a motivated individual, let alone state sponsored agents. The main difficulty with carrying out this type of attack is obtaining a clean image of the required fingerprint. Many fingerprint scanning devices require the user to swipe his / her finger over a horizontal bar, which allows the fingerprint image to be constructed one line at a time; in such cases, the complete fingerprint may not be left on the device, as it would have if the fingerprint scanner had a glass window for scanning the entire finger at once. Regardless, there is a risk that the required fingerprint may be left elsewhere on the phone's case, or that an attacker could obtain fingerprint data from other sources.

Voice recognition technology has been used as a user authentication method on smartphones. For example, Persay's VocalPassword allows users to authenticate to iPhone applications [83] using a previously recorded spoken password [84]. In effect, this system compares two audio clips and accepts the claimed identity if they are similar enough. Obviously, such authentication methods are vulnerable to attack using an unauthorised audio recording of the user's password. A more advanced system could be developed, where the device challenges the user to pronounce a short sequence of random words, with the recording analysed for both accuracy and similarity to the user's typical voice. SentryCom developed a system along similar lines to this [85], although in that case the challenge was to pronounce a randomly generated number. Using numbers is arguably not as strong as arbitrary words would be, since these are easier to spoof using audio manipulation of a relatively small selection of recordings of the victim's speech (e.g. recordings of "one", "two" … "twenty", "thirty", "forty" … "ninety", "hundred", "thousand" and "and").

Some smartphones authenticate users based on a special input sequence on the phone's touchscreen. This pattern of touch inputs is sometimes known as a gesture. Android phones, for example, allow user authentication by the input of a sequence of connected moves on a three by three grid of dots [86]. The rules for this are as follows. The path may start on any dot, and moves between dots can be horizontal, vertical or diagonal, as long as the line between the dots at each end of the move does not pass over a third (unused) dot. (Note that diagonals other than those with a 45 degree inclination are allowed.) Each dot may be visited at most once in the sequence, however dots that have been visited previously may be jumped over to get to an unused dot. The path must be between four and nine dots long, with the password used for authentication simply the sequence in which the dots are encountered along the path (not including dots that are jumped over). With these rules, the number of possible combinations is actually very low, in comparison to a PIN of the same length (see Table 1). There are various rule changes that would expand the number of possible permutations; for example, if the adjacency requirement for moves is removed but the ban on dot reuse is retained, the number of possible *n* dot traversals is $^{9}P_{n} = \frac{9!}{(9-n)!}$, which is a significant improvement. Alternatively, if the adjacency requirement for moves is retained but dot reuse is allowed, then the number of permutations also expands considerably, especially for longer length sequences. Moreover, the relatively small number of permutations available is not the only weakness of this user authentication scheme: Android's gesture based unlocking is particularly vulnerable to "shoulder surfing", since the path chosen is displayed on the screen as it is drawn. (In contrast, a PIN input screen would typically hide the PIN being entered.) In addition, there is the potential for smudges on the screen to reveal important clues about the unlock gesture, which could be helpful for an unauthorised user who has not had the opportunity to observe a live unlock gesture.

Table 1 This table shows the number of possible combinations for Android's gesture based unlocking, on a three by three grid. Note that the number of permutations for the standard Android rules was determined using an exhaustive depth-first search. For the rules allowing dot reuse, the number of permutations was obtained using powers of the adjacency matrix. For the rules allowing non-adjacent moves, the number of possible n *dot traversals is simply* ${}^{9}P_{n}$.

Number of dots in gesture	**Combinations when requiring adjacent moves but allowing dot reuse**	**Combinations without dot reuse but allowing non-adjacent moves**	**Number of unlock combinations when using Android's rules**	**Combinations for equivalent length PIN**
1	9	9	9	10
2	56	72	56	100
3	360	504	320	1000
4	2280	3024	1624	10000
5	14544	15120	7152	100000
6	92448	60480	26016	1000000
7	588672	181440	72912	10000000
8	3745152	362880	140704	100000000
9	23837184	362880	140704	1000000000

While the alternative user authentication methods discussed in this section have their merits, there is none which is reliable enough to be suitable for use as a single factor of authentication. Any one could have value as a second factor of authentication, however, in combination with a password or PIN.

4.1.3 Side Channel Countermeasures

Countermeasures against electromagnetic eavesdropping include improvements to critical hardware to reduce the production of radiation, the addition of shielding to reduce the level of radiation that can escape from the device [43] or the deliberate addition of electromagnetic noise to confuse the signal. (Noise introduction can also make power analysis more difficult.) Such measures do help, but care must be taken if these are to be relied on. This is because these measures do not eliminate the side channel, but merely reduce its signal-to-noise ratio or decrease the intensity of all the emissions (i.e. both signal and noise). An attacker can respond to a decrease in emission intensity by using more sensitive measuring equipment, and deal with noise by sampling a large number of repetitions of the same computation. Since the signal from the computation is always the same but the noise varies between repeats, the noise may be significantly attenuated by simply averaging the signals obtained from the repetitions, or using more advanced statistical analysis techniques [46].

Noise introduction techniques have the advantage that they may be implemented using software or hardware, whereas shielding and other emission reduction strategies must be implemented in hardware. One simple noise introduction strategy on a multicore processor, for example, would be to execute several dummy threads in parallel to the thread performing cryptographic computations, which are deliberately designed to execute random operations (e.g. on a scratch pad in memory that is later discarded) that are difficult to distinguish from the real computation. To be considered effective, noise introduction techniques must increase the number of samples an attacker needs to take to the point where the attacker cannot collect the required number, either because of a limitation placed on the number of re-uses of the secret key or because collection would take longer than the expected lifetime of the device or the information it protects. Alternatively, noise introduction could be considered adequate if it makes the difficulty of using side-channel measurements comparable with the difficulty of a brute-force attack. However, it is important to realise that partial information about a key that is collected through a side-channel can facilitate a brute-force attack by reducing the search space [46].

A refinement of the noise addition approach is to confuse side-channel observations by introducing random delays between successive operations on the bits of the secret key, to make it more difficult for attackers to combine repeated observations correctly [46]. If this were done, then an attacker would be wrong to assume that bit *n* of the secret key is processed at the same time offset from the start of the sequence, in all repetitions. Consequently, a naïve attacker would mix the signal measurements corresponding to different bits of the key when computing the average over several repetitions. In order to overcome this, the attacker would need to be able to analyse the signals to detect special events (e.g. a spike caused by the operation of a CPU clock or data bus) that may be used to synchronise the bits in each repetition.

A natural extension of the above idea is to randomise the order in which bits of the secret key are processed, or write software which is designed to select at random from a multitude of different execution paths when doing computations on critical data [46].

There are also more sophisticated countermeasures for side-channel attacks such as masking, which involves splitting the key *K* into two random keys *K1* and *K2*, such that the exclusive-or of *K1* and *K2* is *K*. A similar splitting operation is performed on the message *M* to be encrypted, yielding *M1* and *M2*. Random permutations of *K1*, *K2*, *M1* and *M2* are then obtained and these are used in a modified version of the DES block encryption scheme [87], obtaining the same result as if no splitting had been used [45].

Most importantly, software developers who write code for cryptographic computations need to be aware of the ways in which its execution could leak information through side-channels. The strongest side-channel signals are obtained from variations in the execution path of the code [46], such as conditional branching instructions. Therefore, software developers should never write code that includes conditional statements examining individual bits of the secret key.

Timing attacks on cryptographic computations may be avoided by a variety of means. For example, the device may be programmed to include a delay between when a cryptographic computation completes and when the response is provided, so that the total time taken is always constant [47]. Alternatively, a random delay could be used. If the delay is implemented by requesting the processor to sleep or perform some repetitive computation (such as executing no-operation instructions inside a loop), then the delay time may be easy to distinguish from genuine cryptographic computation for an adversary with access to the electromagnetic or power analysis side channels [47]. A better solution would be to interleave the genuine computation with the same computation performed using a randomly variable number of random (and bogus) secret keys, with the processor making a random choice as to which of the various computations it will do some work on at each step, and the result only being returned when all the computations are complete. It would then be difficult for an attacker to extract useful timing information based on the overall computation time or to distinguish which parts of the computation are not relevant to the timing attack. A more sophisticated and less computationally expensive countermeasure is to use the technique of blinding, in which the cryptographic operations are performed on input data that has been transformed using a random number, with the result of the cryptographic operation transformed back to the required final answer using the an inverse transformation, based on a number that is related to (and easily computed from) the original random number. As long as the numbers used for these transformations remain secret, the attacker has no knowledge of the inputs to or outputs from the actual cryptographic operation itself. Without this additional information, typical timing attacks are much more difficult [47].

There are a variety of countermeasures for fault injection attacks, as discussed in [49]. One simple technique is to repeat the computation to make sure the same result is obtained both times; this approach may not detect systematic errors, however. Alternatively, the device can verify the result by performing the inverse computation, e.g. taking the cryptographic signature that it computed using the private key and verifying it using the public key. However, for some cryptographic operations this may be computationally expensive. More advanced software based countermeasures have been proposed by Shamir [88] and Aumuller et al [49], whose details are beyond the scope of this report.

Cache based side-channels are a vulnerability that can affect smartphones featuring enclaves operating at different security levels. Eliminating all possibility of such side-channels is not a trivial task and is arguably not possible using software alone [51], however hardware designed with cache security in mind can solve the issue. Possible solutions include the use of a separate cache for each enclave, flushing a shared cache when switching processor control between enclaves, disabling the use of the caching on high security enclaves, preventing security critical threads from executing in parallel to untrusted threads and more advanced techniques such as randomising the mapping between the cache and memory [51].

4.2 Technology for Mixed Professional and Personal Use of Smartphones

4.2.1 Enterproid’s Divide

The many issues surrounding the bring-your-own-device trend have recently spurred the development of new technologies for separating personal and corporate data on smartphones. One is Enterproid’s Divide platform for Android phones (or its derivatives such as AT&T’s Toggle [89]). In this approach, the Divide platform runs as an application within the Android operating system, providing an Android-like enclave in which other Android applications may be installed and kept separate from the host environment [90]. The expected usage is that an Android phone owned by an employee and already containing personal data would have Divide installed on it, which would then be used as a platform for installing corporate applications and which can be given access to corporate networks. It is possible for the Divide environment to be set up to comply with corporate IT and security polices, including the use of a password to switch to the Divide environment if necessary and the ability for the corporation to remotely administer the Divide enclave or wipe the data stored in it (without affecting the data in the host environment) [91]. Corporate data stored in the enclave is protected from access by software in the host environment by encryption, although at present the encryption keys are vulnerable to theft by a rogue process with root access to the device, as the keys are stored in memory [92]. There are plans to prevent this by storing the keys in hardware, which involves a partnership with the chip fabricator Qualcomm. Until this is achieved, the key theft vulnerability makes this product unsuitable for handling sensitive data. On the other hand, this product has the advantage of being available to retrofit on any Android phone brought to work by an employee; the alternative products discussed next require pre-installed software, and sometimes special hardware also.

4.2.2 Redbend's vLogix

A more mature technology is Redbend's vLogix Mobile, where the underlying software on the phone is a hypervisor that runs a number of guest operating systems on separate virtual machines [93]. The hypervisor manages the phone's resources and hardware devices, providing the guest operating systems with virtual interfaces to these so that they can share them without needing to know about the other guests or the hypervisor host. One potential use of this is to install one guest operating system for corporate applications, and another (possibly different) guest operating system for personal use. The separation of the guest operating systems is claimed to be secure, however the only assurance provided is that the product meets a set of standards defined by Redbend itself. Remote administration is possible with this product, using a separate virtual machine that is included for this purpose [94]. Of course, the hypervisor software must be pre-installed on the phone prior to installing the guest operating systems, and so this product cannot be retrofitted to a mobile brought to work by an employee; moreover, it is limited to running on processors based on the ARM Cotex-A15 or Cortex-A7 cores [95].

4.2.3 VMWare's Mobile Virtualization Platform

An alternative is VMWare's Mobile Virtualization Platform [96]. This is also based on virtualisation technology, and allows the creation of separate personal and professional profiles on an Android phone. Like previously mentioned products, the Mobile Virtualization Platform allows the corporation to administer the professional part of the phone, including the ability to wipe only the corporate data from the phone remotely. It is also possible to shut off specific devices such as the camera or Bluetooth [97]. Connection to the corporate network is via a virtual private network, so that the data is protected whilst in transit over the Internet. Separation of corporate phone calls from private ones can be achieved using a voice over IP within the corporate enclave, or by using dual SIM cards. This product thus allows the use of two separate numbers with two different providers, which could be useful for billing separation. One complication of using this product, however, is that it requires the installation of special firmware on the phone by the manufacturer; this therefore limits the use of this product to devices which support it, such as some phones manufactured by LG.

4.2.4 Green Hills Platform for Trusted Mobile Devices

While the above products may be sufficient for commercial use, the security requirements for handling sensitive information in a government context demand some kind of assurance of the reliability of the separation between different enclaves of a phone. One product that provides such assurance is the Green Hills Platform for Trusted Mobile Devices [98]. Functionally, this is similar to Redbend's vLogix Mobile, in that it consists of a hypervisor that hosts an arbitrary number of separated operating systems on the one smartphone. The Green Hills Platform for Trusted Mobile Devices depends on support from special hardware, and so it is only available on phones which are designed to support it; these are not listed in the literature [98].

The main advantage of the Green Hills Platform for Trusted Mobile Devices is that it uses the INTEGRITY-178B Separation Kernel as the hypervisor, which is certified to EAL6+ under the Common Criteria [52, 99]. This certification is arguably more useful than the NSA certifications provided for the General Dynamics Sectéra Edge and L-3 Guardian (see Section 4.3.2), since the Common Criteria allow the assumptions behind the certification to be examined in detail. For instance, the certification for the Green Hills Platform for Trusted Mobile Devices assumes that the level 2 cache is not enabled in the evaluated product ([52], p. 13); it is important to take this into consideration when relying on the product in some particular application, as the level 2 cache could facilitate a covert channel if enabled. If using a device that is based on a closed NSA certification, it is impossible to know if there are any similar assumptions that may have implications for the security of the device, especially under conditions that differ from its original intended use.

There is one function that would be essential to the security of the Green Hills Platform for Trusted Mobile Devices, but which the literature available to the author does not mention. (This could possibly be mentioned in one of the more detailed data sheets that are not available for public download.) This is the ability to detect and / or prevent tampering with the trusted hardware and software on which the hypervisor depends, along similar lines to existing trusted computing products such as the Freescale High Assurance Boot system with its underlying i.MX31 hardware [100]. If tampering could be achieved without triggering an automatic wipe of all enclave data (and without being obvious to the user), then it would be possible for an attacker to modify the hypervisor software or phone hardware to spy on the enclaves, capturing sensitive plaintext that the enclaves store in memory or which are passed to or from input / output devices. For example, a rogue hypervisor could intercept the password used for file system encryption when it is typed by the user or read confidential information written to video memory. Similarly, a hardware Trojan could be inserted into the wires that connect to the phone's keypad or display, reading all data that the user types or capturing pixels displayed on the screen. In order to defend against such attacks, it is necessary to protect all trusted hardware and chips storing trusted software by encasing them, with sensors that detect physical tampering with the case, so that the enclave data can be wiped in that event. Since such detection and wiping requires power, this would also require that the battery be included in the trusted hardware that is protected from tampering. Replacing the battery, therefore, would require a special password protected procedure that temporarily disables the automatic wiping function. Moreover, the battery would need to hold enough energy in reserve for the completion of a wipe operation, with the wipe operation being triggered when this threshold is reached. (Prior to that, it should display a warning and put the phone in low power mode, where it reserves power for monitoring the case sensors and keypad only.) In addition, any updates to the hypervisor software downloaded from the manufacturer would need to be accompanied by a hash, signed by the manufacturer using their private key. The corresponding public key used for verifying the hash would need to be stored permanently on the phone, in a place that is also protected from tampering.

4.3 Smartphone Technology in Government

4.3.1 Vagare

Vagare is a project that was carried out by the Command Control Communication and Intelligence Division of the Defence Science and Technology Organisation in 2007. In short, Vagare trialled mobile phone access to the DSTO Restricted Network for DSTO's senior leadership team. Communication between the smartphone and Defence's network infrastructure was tunnelled over the carrier's network in encrypted form, using an off-the-shelf VPN client. As a matter of policy, Bluetooth was disabled on the smartphone and the Internet was accessible only via the Defence gateway, i.e. not accessible using the carrier's 3G Internet services directly. The smartphones used did not include cameras. There was no specific policy for governing the use of the phones in public places, beyond the existing information security policies of the department, however an unlock PIN was mandatory for authenticating users to the phone's operating system (Symbian). The data stored on the phone was encrypted using PointSec, which meant that users also had to enter a PointSec password in order to access encrypted files on the phone. In addition, an RSA SecureID hardware token was needed in order to produce one-time tokens for authenticating the user on the DSTO DRN. These three different authentication methods were essential for security, since the system consisted of several different components from different vendors that could not share authentication information.

The Vagare trial was seen as being mostly successful, with many users finding mobile DRN connectivity convenient. However, some users were frustrated by the multiple layers of authentication, especially the need to remember an unlock PIN and a PointSec password. Ultimately the trial ended and was not extended, as it was not seen to be prudent to continue to allow DSTO to use a system that was not accredited for widespread deployment. For further information concerning Vagare, please contact Julian Costa or Peter Shoubridge at DSTO.

4.3.2 Existing US Government Approved Smartphones

There are some commercial smartphones that are already available for use in handling sensitive information, including information at different classifications. For instance, the General Dynamics Sectéra Edge and L-3 Guardian are both considered to be Secure Mobile Environment-Portable Electronic Devices, that are authorised by the NSA to handle information up to the classification SECRET in the USA [101]. They are 3G devices based on the Windows Mobile operating system, that were developed with high security environments in mind; as a result, these devices are extremely expensive in comparison to more common commercial-off-the-shelf smartphones.

Note that the L-3 Guardian is able to handle data at both UNCLASSIFIED and SECRET levels, being authorised by the NSA to connect to both the NIPRNET and SIPRNET [102]; however, the device is not certified under the Common Criteria, which would be more useful in assessing the suitability of this device for use in an Australian Government context. Moreover, it is not clear if this device allows as many security domains as could be needed, such as UNCLASSIFIED (personal), UNCLASSIFIED (professional), RESTRICTED, CONFIDENTIAL and SECRET.

The General Dynamics Sectéra Edge is likewise authorised by the NSA for connection to NIPRNET and SIPRNET, rather than being certified under the Common Criteria. However, the Sectéra Edge has the additional feature of being authorised by the NSA to carry TOP SECRET level voice data [103].

There is also an Android phone which is certified for handling US Government information. Dell's Streak 5, running Android 2.2, is certified by the Defense Information Systems Agency for UNCLASSIFIED level use in the Department of Defense [104]. Approval was granted on the 28th of October 2011 [105] following a project that began work on hardening the existing Streak 5 in September 2010, with the certification process beginning around June 2011 [104]; this demonstrates the delays that are typical for certification, even for devices intended to operate only on UNCLASSIFIED information. While the Streak 5 is no longer available to commercial customers, Dell is still supplying it to the Department of Defense since they are a sufficiently large customer [104].

4.3.3 Development of NSA Secured COTS Smartphones

Owing to the long delay and huge expense associated with developing and certifying smartphones for handling classified government information, there is a strong incentive to find ways in which Commercial-Off-The-Shelf technology can be safely utilised for this purpose. There have been reports in the media [106] of research by the NSA, aimed at creating a smartphone that is secured for handling United States' national security classified information. Further details have emerged more recently [101], which clarify that the project is mainly concerned with determining the configurations that are necessary for securing commercial grade smartphones. An unclassified version of the specification document has been released [107], which is a useful source of information and advice, much of which is too detailed to be within the scope of this report. Trials of NSA configured commercial smartphones are currently underway, and in future the NSA will develop partnerships with technology companies to discuss how smartphones may be adapted to better suit government needs [101].

Of particular interest in the NSA report is the section concerning the security of the operating system and application environment ([107], pp. 14-33). This provides detailed advice about the security capabilities required in a mobile operating system, including the configuration settings that should be available, the notifications that should be provided to warn the user about potentially dangerous settings, security monitoring, device management, trusted processes, key storage and the proper use of a VPN client to connect to classified networks.

For all its merits, the NSA report is however somewhat lacking in that it neglects to discuss side channels such as power analysis and electromagnetic emissions, which are crucial to the security of information stored on or transmitted by mobile devices. It is possible, of course, that the NSA research does consider such matters, but has not included this research in the publicly released report for security reasons or because the research was not advanced enough for inclusion in the initial release.

The current NSA specification also includes no discussion of the issues that arise when a single device is required to handle information at different classification levels. This is an issue, because many users in the defence and intelligence community must handle information at classifications ranging from unclassified to top secret, with several classifications in between, as well as security compartments for specific projects that are on a need-to-know basis. If this information is to be available from a smartphone, then the device must be capable of connecting to a variety of different secured networks at various classifications, without leaking any information from a higher classification to a lower classification, or allowing malware from an unclassified network to propagate to a classified network. However, there are plans to extend the research to consider these issues [101].

A collaborative effort is also underway involving the NSA and George Mason University, which aims to produce a hardened version of the Android 3.0 kernel that is certified to handle SECRET level information [108]. It is not clear if this project is connected to the aforementioned NSA research or not. As of the 11th of October 2011, the hardened kernel had been built and was undergoing certification for Federal Information Processing Standard 104-2, with certification expected to be completed very soon afterwards; it is not clear what the present status of this project is. While FIPS 104-2 certification is not sufficient for handling classified information, it is one of the necessary pre-requisites. There are plans to complete the other required certifications, such as of the kernel's implementation of the Secure Socket Layer, and so extend its authorisation to handling classified data up to SECRET level [108].

4.3.4 Existing Australian Government Approved Smartphones

The US has a major advantage over Australia when it comes to the accreditation of ICT products: Australian Government departments, agencies and defence forces are much smaller buyers of technology than their US counterparts, which reduces their ability to influence commercial decisions. This is particularly important in regards to smartphones, in that the delays involved with accreditation are significant in comparison to the normal commercial lifetimes of the products, and so obtaining a useful lifetime for an accredited product may depend on negotiating a lifetime extension on an obsolete product. The most obvious approach to this problem is to restrict Australian accreditation efforts to devices that are already accredited in the US, or in the process of being accredited, to maximise the chance of accredited products being available for a long time in order to service the US market. This also allows time and money to be saved on the accreditation process, since it may draw on research that has already been completed. On the other hand, there is a risk that limiting accreditation efforts to devices favoured by the US may mean that valuable technologies are overlooked, some of which may be eminently suitable for Australian Government use.

There are some smartphones and related products that are currently certified by DSD for use in the Australian Government. The complete list of certified ICT products is available online [109], along with links to more detailed information including the restrictions placed on their use.

The smartphone which is most highly certified is the Blackberry (versions 5, 6, 7 and 7.1) , which is authorised to handle information at classifications of UNCLASSIFIED, X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE), RESTRICTED and PROTECTED. When the device is turned off or locked, the device itself may be handled as an UNCLASSIFIED item. Also certified is the BlackBerry Enterprise Server software (versions 4.1.3-4.1.6 and 5.0.0–5.0.3), which is an essential part of the system when running a fleet of BlackBerries. There are however special restrictions on its use, so that a BlackBerry is not authorised for making or receiving classified voice calls or text messages. In addition, the dual personas feature was not evaluated, and so this must be disabled by policy on the BlackBerry Enterprise Server if this allows connections to a PROTECTED network [109]. This is an unfortunate limitation, as the dual persona feature provides separate personal and professional usage modes for the device, avoiding many of the issues discussed earlier.

Windows Mobile 6 has also been certified by DSD, but only for handling UNCLASSIFIED, X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) and RESTRICTED information. Since no encryption is used for the data stored on the device, the device itself must be handled at the same level as the highest classification network it has been connected to. Windows Mobile 6.1 has also been certified for handling UNCLASSIFIED, X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) and RESTRICTED information. Since Windows Mobile 6.1 introduces file system encryption, there is the possibility that, in future, mobile devices using that operating system will be able to store classified information without the mobile devices needing to be handled as classified material. However, as the encryption is still being evaluated this is not yet the case. Currently, a smartphone running Windows Mobile 6.1 may be handled as an UNCLASSIFIED item if it stores only X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) or UNCLASSIFIED information; however, if it is connected to a RESTRICTED level network then it must be handled as a RESTRICTED level item [109].

Strictly speaking, the targets of evaluation for the Windows Mobile certifications explicitly exclude the hardware on which it runs, including only the software from device drivers upwards [109]. This means that, although the Windows Mobile operating system itself is authorised to handle classified data, the hardware on which it runs may not be. In fact, as far as the author can see, no mobile phone hardware apart from the BlackBerry (and possibly the iPhone) have yet been evaluated by DSD, so it could be argued that the Windows Mobile certification does not really allow anything as there is no certified hardware on which it can be run. This situation is confusing and should be clarified. If the Windows Mobile certification does provide a de-facto authorisation for it to be used on some set of standard hardware then this should be stated explicitly, with the list of approved hardware provided. If not, then this should be emphasised; moreover, some smartphone hardware platforms would need to be evaluated, in order to make the Windows Mobile certification useful.

The more popular commercial smartphones are less well represented on the list of approved products: no Google Android products have yet been certified by DSD. However, DSD has released a detailed guide for security hardening Apple iOS based products, including the iPhone. This document provides official permission to use iOS 5.1 or higher for handling information at classifications of UNCLASSIFIED, X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE), RESTRICTED or PROTECTED, providing that the strictures of the guide are followed [9]. Such a device may be handled as UNCLASSIFIED material. (There is also permission granted to use iOS 4.3.3 products and higher to access information at UNCLASSIFIED and X-IN-CONFIDENCE (excluding CABINET-IN-CONFIDENCE) levels, providing that an earlier security hardening guide is followed [37]; however, the guide also includes a disclaimer that "this document does not constitute a DSD certification or formal evaluation of iOS".) While the focus of the iOS 5.1 certification is on the operating system itself, the specific hardware devices that it applies to are listed as the iPod Touch, iPhone and iPad [9], so the ambiguity that applied to the Windows Mobile certification is less of an issue here. However, if it is intended for the certification to apply to all hardware versions of these devices, then this should be stated explicitly; otherwise, a more specific list of certified hardware platforms should be provided.

Note that the iOS hardening guide acknowledges ([9], p. 1) that it is not possible to meet all the requirements of the Australian Government's information security manual [110] in iOS 5 by using technical controls alone. Hence, the iOS hardening guide also includes risk mitigation measures in appendix E, such as educating users in how to avoid dangerous actions that could compromise the device or information stored on it. This reliance on user education and compliance is potentially a little dangerous. Moreover, there is one policy in the information security manual which is not supported in iOS 5 and is also not mentioned in the iOS hardening guide: this is the requirement that PROTECTED information accessed using a non-agency owned mobile device must not be stored on the device ([110], Control 0693, p. 269). It could reasonably be argued that this requirement should not apply to information stored in encrypted form, however that is not what the information security manual actually says. This being the case, either the information security manual needs to be changed to allow the storage of PROTECTED information on non-agency owned devices if it is encrypted, or appendix E of the iOS hardening guide needs to be changed to tell users to avoid storing PROTECTED information on their personal iOS devices (even if the device has been security hardened to DSD standards and stores PROTECTED information in encrypted form).

As a more general comment, it would appear that there is considerable pressure from users in government for the certification of popular models of smartphones. With a wide variety of models in use and new models being released all the time, the inevitable certification delays and limited number of certifications that are feasible will always mean that users are disappointed about the range of certified smartphones available. Meanwhile, the pressure for speedy certifications creates an incentive that is contrary to the aim of obtaining a thorough assessment of the security risks. These issues are a strong motivation for finding an alternative to certifying COTS smartphones and operating systems, such as using a hypervisor system to allow non-certified operating systems to be used in separated enclaves of a smartphone (see Section 6.1) or using trusted input / output devices that use a VPN connection to a secure network through an untrusted and uncertified smartphone (see Section 6.2.3).

5. Review of Existing Practices and Policies for Professional Use of Mobile Platforms

5.1 Private Industry

The traditional model for the professional use of mobile platforms is for companies to supply employees with devices that are selected, owned and administered by the company. There are obvious security benefits to doing this, such as the existence of a uniform operating system and application environment (which simplifies the task of IT administrators), the ability for IT staff to roll out software updates across the fleet and the ability to prevent users from modifying critical security settings or installing potentially dangerous applications [111].

In recent times, there has been increasing pressure from employees to be allowed to use their own mobile devices for professional purposes, especially smartphones [111]. This is partly because employees do not like the inconvenience of carrying a professional device as well as a personal one, and partly because workplaces frequently use older models and operating systems that the company's IT staff have had time to evaluate and develop tools and procedures for supporting. Moreover, traditional favourites of the corporate world, such as Windows Mobile and Blackberry, are falling out of favour with users, who increasingly prefer iPhones or Android phones [112, 113].

There is a clear need for corporations to develop policies for managing the bring-your-own-device trend. However, a recent survey of Australian legal and accountancy firms found that only 10% had formal strategies in place for dealing with this issue [114], which suggests that the corporate world will struggle with it for some time to come. There is nothing like a consensus emerging; however, some policies that are in use and ideas that have been put forward are the following. Some of these statements have been paraphrased for clarity. They do not necessarily represent the views of this report's author, and their advice is not necessarily applicable in an Australian Government context.

- If an organisation does not develop a bring-your-own-device policy, but instead insists on the status quo of the traditional model, there are risks that staff will become frustrated, potential working hours will be lost and productivity will suffer. (Rick Ness, Thomson Reuters' chief technology officer [114])
- If it is necessary to access sensitive information from a mobile device, that information should be stored in and accessed from a separated 'sandbox' on the device, with encryption used to protect the data. It must also be possible to wipe that 'sandbox' remotely, without affecting personal data stored outside of the sandbox. (Paul Greenwood, CIO of Clifford Chance [114])
- In developing a bring-your-own-device policy, it is necessary to find the right balance between clarity and complexity. It is also important to achieve the correct level of control, as a policy which is too tight could drive bring-your-own usage underground, which is much worse than a well managed compromise. Devices used for handling company data must meet a minimum set of security standards, which include data encryption, password protection and user lockout after 5 failed password attempts. When employees lose custody of the device the phone's data must be wiped, however this must be specified and agreed to in advance. (Ian Jansen, CIO of Dimension Data [114])
- Corporations who traditionally rely on Microsoft Windows can use virtualisation software in order to allow their normal application environment to be run on mobile devices brought by employees. Some examples of companies that do this are Jetstar, EMC and the Commonwealth Bank [115].
- Despite challenges relating to security, support and data ownership, employers are beginning to see a liberal bring-your-own-device policy as an employee attraction and retention strategy. Allowing employees to bring their own devices increases employee satisfaction, whilst saving money that would have been spent on corporate-issued devices that employees may not like. Some devices which users often bring, such as Apple products, have a more intuitive user interface, and so IT support costs may fall as a result of a bring-your-own device policy. (Leanne Ward, vice president of IT outsourcing and support services, Unisys Asia Pacific [115])
- IT departments will either need to add support for the devices that employees bring or use virtualisation to allow corporate applications to function on different platforms. Either way, some extra support costs will be introduced, however there may not be a net increase in costs, since benefits such as peer-support behaviour and improved productivity are also introduced. (Steve Hodgkinson, research director of research firm Ovum [115])
- "Employees and IT managers are simply not prepared for a world running on handhelds. … A sound corporate policy might start with the simple mandate of locking and secure passwords for mobile devices and a loss-prevention security

system that locks and wipes the device if it gets lost or stolen.” (Michelle Savage, spokesperson for NetQuin, a US provider of mobile security products [116])

- "We'll allow staff to use any device to access systems, though we'll retain strict control within secure networks by enforcing port-level security, encryption, multiple passwords, auto lockouts and 802.1x authorisation regardless of wired or wireless. Networks are segregated based on security requirements." (Matthew Toohey, general manager of information services at iiNet [116])
- “Keeping malware out of a system is done through user education, not software.” (Sean Greene from Evidence Solutions, a US data recovery company that allows employees to bring Android devices to work [116])

While there are some valid points raised by the above representatives from industry, there are significant variations in the policies and approach taken to incorporating employee owned mobile devices into corporate systems. This is partly because many issues involved are still matters for discussion, and partly because choices which are appropriate for one company may not work well in another, if they have dissimilar business systems and different workplace cultures. Despite this, there is much that may be learned from the experience of industry when setting government ICT policies.

On the other hand, the security requirements of government differ to those of private industry, since governments have a greater responsibility to protect the confidentiality of sensitive data in their care; in some situations, lives may even be at stake. For this reason, governments typically need stricter policies than private industry for controlling the use of mobile devices that handle sensitive data.

There are also potential problems if governments choose ICT policies that are too strict. Governments and private industry alike are subject to pressure from employees for permission to bring their own devices to work. Since governments must compete with private industry in the employment market, with a limited supply of skilled workers available, recruitment could suffer if high-calibre prospective employees choose to work elsewhere as a result of restrictions on profession use of their smartphones. This is an important consideration for the long term success of government organisations.

5.2 US Government

There is a significant overlap between the issues facing the Australian Government and those facing the US Government, in regards to smartphone usage policy. However, the Australian Government has different legislative requirements for national security, as well as a different division of security responsibilities between various government agencies. Hence, US policy should be considered as a useful reference and a checklist of things to consider for Australian policy, not a standard that should be copied without due consideration of the differing legislative and operational environment in Australia.

5.2.1 Non-National Security Advice

The National Institute of Standards and Technology offer documents for public download on a wide variety of computer security topics [117], ranging from cryptography and security protocols to digital forensics. While these are not legally binding standards even in the US, they are nevertheless a useful resource. Of particular interest is a report on mobile phone security [118], which discusses many of the threats identified in this report, as well as appropriate policy responses. There are also a number of more technical documents that are relevant, such as the guide to virtual private networks [119], since VPNs are the preferred approach to connecting smartphones to sensitive networks over the untrusted communication channel provided by the carrier.

5.2.2 National Security Policy and Advice

The National Institute of Standards and Technology also provide standards [120] for certain aspects of computer security, such as cryptography and authentication, which are mandatory for US Government departments and agencies. These are known as the Federal Information Processing Standards (FIPS). While there are no FIPS relating to smartphones specifically, many of the security functions of smartphones can be evaluated against these standards, especially the standards concerning cryptography [121]. In addition, FIPS190 [122] includes an extensive discussion of user authentication, especially password policy; however, this document is deficient in some respects, e.g. in that it mentions the need to store password hashes rather than the plaintext passwords but does not acknowledge the need for salting them (to prevent cracking by means of rainbow tables). FIPS 201 [123] is a more recent standard covering personal identity validation, however the main focus of this document is on the use of token (smartcard) based authentication systems, which are not relevant to most smartphones.

The Defense Information Systems Agency also provides public access to a range of security standards that are mandatory within the US Department of Defense specifically, under the authority of Department of Defense directive 8500.1. There is a section of these standards that are concerned with the security of mobile devices such as smartphones [124], which includes documents concerning appropriate security configuration and usage conditions of general mobile devices, as well as for Android phones, iOS devices, Blackberries and Windows Mobile devices specifically. There are also documents on security topics of particular concern, such as appropriate configuration of devices with Bluetooth capabilities [38]. Of particular interest is the checklist of security requirements that Department of Defense smartphones are required to meet [125], which could be a valuable reference for Australian Government policymakers. This document covers the areas of email access from smartphones, stored data protection, transmitted data protection, public key infrastructures, over-the-air provisioning of new applications, web browsing, unlock passwords, application controls, Bluetooth settings, WiFi settings, security policy enforcement and malware detection and prevention.

5.3 Australian Government

5.3.1 Current National Security Policy

The primary reference for current policies that apply to smartphone usage is the Australian Government Information Security Manual [110], especially the section from page 268 to page 276. The following are the key policies; *italics* are used to indicate the author's comments:

- Control 1082: It is the responsibility of specific government agencies to develop policies for the use of mobile devices. *At this point, the policy should add that the agency must communicate this policy to all employees who need to use mobile devices for professional purposes.*
- Control 1195: Agencies should use a Mobile Device Management solution to ensure their mobile device policy is applied to all mobile devices used with their systems. *This policy may work well with mobile devices issued by the agency, but could be difficult to apply to mobile devices owned by employees. Employees may own a variety of different types of device, many of which may not be compatible with the chosen Mobile Device Management solution. Moreover, this solution will require the employees to grant administrator privileges to the agency for this purpose, which some employees may not be willing to do. In addition, users would also need to relinquish administrator privileges if the agency requires certainty that key security configurations have not been reversed by the employee; this would subsequently prevent users from installing new applications, which some employees may not find acceptable.*
- Control 1083: Employees must be made aware of the maximum classification of data that is permitted to be accessed from mobile devices under the agency's policy.
- Control 0687: TOP SECRET information is not to be processed or stored on mobile devices, unless permission is first obtained from DSD.
- Control 1047: Mobile devices not owned by the agency may be used to connect to UNCLASSIFIED government networks, but if they do they should use a trusted operating environment that prevents sensitive information from being stored on the device.
- Control 0693: Mobile devices not owned by the agency may be used to connect to classified government networks up to PROTECTED level, but must use a trusted operating environment if they do; moreover, the operating environment must prevent classified information from being stored on the device
- Control 0694: Mobile devices not owned by the agency must not be used to access networks classified CONFIDENTIAL or higher.
- Control 0172: Agencies must not permit non-agency owned mobile devices to be brought into TOP SECRET areas without prior approval from the accreditation authority.
- Control 1297: Prior to allowing non-agency owned mobile devices to connect to an agency system, agencies must seek legal advice.

- Control 0869: A DSD approved cryptographic algorithm should be used to encrypt all information stored on a mobile device.
- Control 1084: If stored data is not encrypted, then the mobile device must be handled as a classified asset. *At this point, the policy should say that the non-encrypted mobile device is to be handled at the same level as the highest classification data on it.*
- Control 1085: Encryption must be used when communicating classified information over public networks. *At this point, the policy should say that encryption is also to be used when transmitting information over a government network at a lower classification.*
- Control 1145: The use of privacy filters is recommended for the screens on mobile devices.
- Control 0682: Bluetooth must be disabled on mobile devices that handle information classified CONFIDENTIAL or higher.
- Control 1196: Mobile devices handling information at classifications up to PROTECTED must remain undiscoverable to other Bluetooth devices except during pairing.
- Control 1198: Mobile devices handling information at classifications up to PROTECTED must not be paired by Bluetooth to devices other than the one intended. *While this is a valid aspiration, it is not possible to apply this control with certainty; in future, a vulnerability may emerge that allows man-in-the-middle attacks on Bluetooth devices that have been configured according to all the recommendations. Hence, prohibiting unintended pairings as a control is similar in utility to stipulating that government computer networks should not be able to be hacked. This control should be removed or changed into justification text for specific, implementable controls that work towards this goal.*
- Control 1200: If mobile devices handling information at classifications up to PROTECTED are configured to use Bluetooth, this must be Bluetooth version 2.1 or later.
- Control 1201: If mobile devices handling information at classifications up to PROTECTED are to use Bluetooth, the device must be configured to support a single Bluetooth headset connection. *This control is ambiguous; it could mean that a single Bluetooth headset connection is the only Bluetooth connection allowed, or alternatively it could mean that having exactly one Bluetooth headset connection is mandatory, with Bluetooth connections to other types of device being valid options. This should be clarified.*
- Control 1199: Mobile devices handling information at classifications up to PROTECTED should only participate in Bluetooth pairing if this is required for business needs. Bluetooth pairing should only remain enabled on the device as long as the business case for this continues to exist.
- Control 1197: Mobile devices handling information at classifications up to PROTECTED should be configured to allow only those Bluetooth classes that are required. *This control should specify that a business need must exist, rather than simply*

saying "required". It may also be worthwhile to rewrite this control to highlight the fact that there is a hierarchy of Bluetooth classes, so that a business need that justifies the use of Bluetooth class 2 automatically justifies Bluetooth class 3 (but not class 1), for example.

- Control 1202: Bluetooth headsets handling information at classifications up to PROTECTED should be configured to use only class 2 and / or class 3 Bluetooth connections, so that the communication range is limited to at most 10 metres.

- Control 0862: The configuration of mobile devices should be controlled by the agency.

- Control 0863: The agency must prevent users from installing or uninstalling applications on mobile devices.

- Control 0864: The agency must prevent users from disabling security functions on mobile devices.

- Control 1049: The agency should ensure that security updates are applied to mobile devices on a regular basis, and test them regularly to ensure they are still secure. *How regularly do these things need to be done? What tests should be done?*

- Control 0874: The agency should not allow mobile devices to connect to the Internet except when temporarily connecting to facilitate the establishment of a VPN connection to a government network. *The use of the word "temporarily" here is misleading; the Internet connection must remain live throughout the entire duration of a VPN session, otherwise there is no channel available through which encrypted information may be tunnelled. Hence, there will be significant exposure of the device to the Internet whatever this policy says, and any device which stores plaintext government information or the keys to access encrypted government information must be secure enough to withstand attacks from the Internet. That said, there are advantages to limiting Internet access to the VPN client, for example by mandating the use of a firewall which blocks all TCP ports except those used by the VPN client. It may also be advisable to close the Internet connection entirely when the VPN client is not in use. However, for devices with separate personal and professional enclaves, limits on Internet access should be applied to professional enclaves only.*

- Control 0705: The agency must disable split tunnelling when using a VPN connection from a mobile device to connect to a government network. *Whether split tunnelling is enabled in the VPN application or not, the untrusted Internet connection to the mobile device must still exist in order for the VPN to use it; therefore, this connection is still a potential line of attack. At best, this control may help reduce the user's exposure to the open Internet, for example by forcing web browsing activities to take place through the agency's proxy server rather than directly.*

- Control 0240: Paging, MMS, SMS or instant messaging services must not be used to communicate sensitive or classified information. *There is no mention here or elsewhere in this section of controls on communicating classified information by voice. It would make sense to include a control that prevents users from using unsecured voice services for communicating classified information. A voice over IP application through the VPN would be more appropriate for communicating classified information.*

- Control 0700: Agencies should develop an emergency destruction plan for mobile devices handling sensitive information with any classification between UNCLASSIFIED and PROTECTED, inclusive. *Under what conditions are emergency destruction plans to be executed? Also, for devices with separate personal and professional enclaves, the emergency destruction plan should not apply to personal enclaves.*
- Control 0701: The agency must develop an emergency destruction plan for mobile devices handling information with a classification of CONFIDENTIAL or above. *Under what conditions are emergency destruction plans to be executed? Do these conditions differ for contents classified CONFIDENTIAL or above? Also, for devices with separate personal and professional enclaves, the emergency destruction plan should not apply to personal enclaves.*
- Control 0702: The emergency destruction plan for mobile devices handling information with a classification of CONFIDENTIAL or above must use a cryptographic zeroise or sanitise function of cryptographic keys stored on the mobile device, if one is available.
- Control 1086: Mobile devices should not be used for personal non-business use or by people other than those specifically authorised. *This should be reworded to allow for dual-use phones with separate enclaves. E.g. "Government owned mobile devices without a separate personal enclave should not be used for personal non-business use or by people other than those specifically authorised. However, if a government owned mobile device has appropriately certified separation between enclaves for handling professional and personal data, then the personal enclave only may be used by the authorised user for non-business purposes; the professional enclave is not to be used for personal non-business use or by people other than those specifically authorised."*
- Control 0866: The agency should ensure that employees are aware not to access or communicate sensitive or classified information when in public locations, unless extra care is taken to reduce the chance of being overheard or having the screen of the device observed. *No precise definition of a public location is given, although the examples given are useful. Also note that there are some new technologies which could allow some types of mobile device use in public locations, without a significant risk of classified data being exposed. See Section 6.2.1.*
- Control 0870: Mobile devices are to be carried in a secured state when not being actively used.
- Control 0871: Mobile devices must be kept under continual direct supervision when in use.
- Control 1298: The agency should implement technical controls on mobile devices and conduct user education prior to personnel travelling overseas with a mobile device. *This is rather vague regarding the technical controls that should be implemented. The content to be covered in the user education should also be specified, e.g. by referring to specific sections of the Australian Government Information Security Manual and / or other documents.*
- Control 1087: Mobile devices must remain in the custody of the user at all times when the user is travelling. *An exception to this must be made for employees visiting overseas defence facilities, where the user may be required to put the device in a locked*

cabinet before entering. There may be other circumstances in which retaining the device is not practical, so the controls should specify alternative means by which mobile devices may be physically secured.

- Control 1299: This control specifies a range of precautions that employees should take when travelling overseas with a mobile device containing sensitive or classified information. *The suggested controls are sensible but the request for employees to clear the web browser temporary data after every session is unduly onerous. It would be better to require browsers to be configured to clear this data automatically each time the browser is closed.*

- Control 1088: If travelling personnel are requested to decrypt mobile devices for inspection by customs personnel, or their mobile device leaves their possession at any time, then the member must report the potential compromise of information on the device to an Information Technology Security Manager as soon as possible. *This should be generalised to something like: "Mobile device users are to report any potential compromise of the device to Australian Government authorities as soon as possible." The specific example relating to customs personnel should be retained for illustration. A control could also be added, stipulating that a "panic password" should be configured on the phone if this feature is available, which sanitises the device when entered at the login screen. In circumstances such as this the panic password should be provided to the customs personnel or entered by the owner, thereby reducing the chance that sensitive data will be compromised.*

- Control 1300: Upon return from overseas travel, agency employees should change all passphrases associated with a mobile device that was taken with them.

- Control 0865: Mobile devices are only to be used in environments that meet the minimum physical security requirements in the Australian Government Physical Security Management Protocol. *Again, there are some new technologies which could allow some types of mobile device use in locations that do not meet these requirements, without a significant risk of classified data being exposed. See Section 6.2.1. In addition, the link between this control and control 0866 should be clarified, in order avoid any apparent contradiction.*

- Control 0685: Mobile devices that are not in use must be secured in accordance with the minimum physical security requirements in the Australian Government Physical Security Management Protocol. *If the encryption used for the device is adequate, then it may be handled as an UNCLASSIFIED item and as such, should not have any specific storage requirements. If the mobile device is not sufficiently secure that it may store classified material without being considered a classified item, then of course this control is necessary. However, the distinction between these two cases should be made.*

As a more general comment, the policy is needlessly complex and ambiguous regarding the use of privately owned mobile devices for conducting government business. Controls 1047, 0693 and 0694 are too complex, in comparison to the obvious alternative of banning the use of privately owned mobile devices from handling government information altogether. In addition, it is not clear how the various controls relating to the device configuration, the application environment and emergency destruction should be applied to a privately owned phone used for professional purposes, and attempting to enforce these policies on private smartphones could lead to conflicts with employees. Moreover, control 1086 conflicts with the earlier controls that implicitly allow devices not owned by the agency to be used for handling classified information. According to a strict interpretation of the policy, an employee is allowed to use a mobile device that he / she owns for accessing government information up to PROTECTED level, but from that time on must cease using the mobile device for personal purposes. In this case, the user has effectively provided a mobile device for dedicated professional use at his / her own expense. This could lead to problems, especially if employees are not aware of this policy before making the decision to use a personal mobile device to access government networks.

5.3.2 Future Policy Objectives

There are aspirations among Australian Government policymakers for increased access to government information from mobile devices. For example, a 2010 report from the Chief Information Officer Group within the Department of Defence [126] identifies the following future needs:

- Allow mobile access to defence applications and data from any device, anywhere and at anytime. This includes access from devices that are not owned or administered by Defence and access from overseas locations.
- Ensure that any changes to policies and practice satisfy the security requirements associated with handling classified information.
- The level of access provided when using a mobile device should be the maximum that security considerations permit, given the type of device, the extent to which Defence can control the device and its location at the time of use.

In order to meet future needs, the CIOG report recommends the following:

- Mobile devices are to be categorised as Defence trusted devices (i.e. devices owned and administered by Defence), personnel trusted devices (i.e. devices owned and / or administered by Defence employees) and untrusted devices. Different security polices will apply to each.
- Highly certified Defence trusted devices will be allowed access to Defence networks up to SECRET level.
- Lesser certified Defence trusted devices and personnel trusted devices will have more limited privileges, e.g. connecting only to UNCLASSIFIED and in some cases RESTRICTED networks.
- There will be a Defence Data Centre, which manages classified and unclassified data, a suite of applications that are common throughout Defence and includes some centralised processing capability. In other words, the Defence Data Centre is a kind of cloud service managed by Defence.
- Access to Defence Data Centre applications will be via the Next Generation Desktop, in order to provide a consistent user interface on a range of different devices.

There are potential dangers with these policy objectives. In particular, it is risky to place any level of trust in mobile devices that are not owned and administered by the relevant government agency, in this case Defence. The reasons for this are discussed at length in Section 3.2.3 of this report and will not be repeated here.

While the author believes that the Defence Data Centre and associated Next Generation Desktop are worthwhile projects for streamlining general ICT usage, it should be acknowledged that complete centralisation of Defence applications will never be possible. There are many specialist desktop applications which are essential to the operations of parts of Defence but which may not be cost effective to integrate into the Defence Data Centre. For example, specialist computer aided design and analysis software is essential for certain engineering activities within Defence, but is not required by most users; providing such software to all users of the Defence Data Centre would be prohibitively expensive. This issue could be solved by purchasing a much smaller number of licenses for the Defence Data Centre, with one of the licenses being taken every time a user opens a new instance of the software and then relinquished when the user closes the instance. However, having a pool of licenses in common to an organisation as large as Defence is a system that is open to abuse, for example by a user who tries to reserve a license permanently by keeping the software open.

Another issue with restricting users to software from a common operating environment is that some specialist research activities require software (for example hacking tools and malware) which is not appropriate or safe for the general user base. Moreover, many research activities in Defence need to occur on non-standard hardware, in non-standard operating systems, on standalone computing platforms or utilising custom developed software.

6. Recommendations for Future Australian Government Policy and Further Research

6.1 Policy Recommendations

The following are the author's recommendations for the use of smartphones within the Australian Government:

1. Any mobile device used for handling government information above UNCLASSIFIED should be purchased and owned by the Commonwealth, in order to avoid any contention over the administrative rights to the device. It also allows the Commonwealth to select products with the required level of secure separation between personal and professional enclaves.
2. The use of privately owned devices for handling government information above UNCLASSIFIED should not be allowed. This is consistent with existing policy ([110], Control 0694, p. 269), as far as information classified at CONFIDENTIAL

and above is concerned, since this is currently banned from privately owned devices. However, classified information up to PROTECTED level can be accessed from but not stored on privately owned mobile devices under the current policy. The author believes that it would be better to simplify the policy by prohibiting access to all classifications of government information (except UNCLASSIFIED) from privately owned mobile devices.

3. There is one exception where privately owned mobile devices should be allowed to handle government information, which is if special hardware is added to make access safe, along the lines of the TRIODE system discussed in Section 6.2.3. In that case, privately owned mobile devices would need to be allowed to transmit and store classified information (possibly at levels as high as SECRET), but only in encrypted form and where a key is required for decryption that is never stored on or processed by the privately owned mobile device. That is, a privately owned mobile device should be considered to be an untrusted component, just like a public Internet router, which the government does not have the ability to control and which may be used only for tunnelling encrypted data between trusted devices. Such a mobile device should not be subject to any government security policies and should also be allowed to be used for personal non-business use or to be used by individuals other than the intended user.

4. Users should be given some very limited range of choices for their work smartphone, from a pre-approved list of devices and operating systems that have been vetted by communications security experts and customised as required. For cost limitation purposes, it may be necessary to limit the choices to just one selection of smartphone and underlying operating system, although hypervisor based systems would allow the user complete freedom to choose the operating system installed in the personal enclave. However, it is important that such a list is subject to review on a regular basis, in order to assess newly available technologies that may enhance the secure handling of Commonwealth information and take account of emerging threats and vulnerabilities.

5. The operating system on any phone used for handling government information must be capable of secure segregation of personal and professional use, at the very least as far as separating data and the application environments are concerned. Ideally, a hypervisor system should be used to manage separate personal and professional enclaves, including professional enclaves at several different classifications if necessary. In a government context, the only hypervisor known to the author that provides sufficient assurance of secure separation is the Green Hills Platform for Trusted Mobile Devices, with an EAL6+ rating under the Common Criteria (see Section 4.2.4). Further research should be done to confirm the suitability of this product prior to adoption, however, especially regarding tampering detection and resistance to side channel attacks. Ideally, the whole system should be certified, although that certification could draw heavily on the existing certification for the hypervisor.

6. Alternatives to the Green Hills Platform for Trusted Mobile Devices include the General Dynamics Sectéra Edge and L-3 Guardian, which are authorised by the NSA to access US Government data at unclassified and secret levels. However, it is

not clear if these devices can be configured to use a sufficient number of separated domains for the full range of possible uses in an Australian Government context. These products also do not have the ability for arbitrary selection of enclave operating systems, this being Windows Mobile for all enclaves including the personal one. Moreover, the detailed documentation relating to the NSA certification of these products is not publicly available, making it difficult to assess the suitability of these products for Australian Government use.

7. On a hypervisor system, it is necessary to trust the mechanism for switching between the different enclaves. Ideally, this should be achieved using physical buttons to scroll between the different enclaves, with a small trusted display (separate from the main screen) indicating which enclave is active, so that a user could detect an attempt by rogue software on a low level enclave to impersonate a higher level enclave. (Note that it is too limiting to use distinct buttons to select each enclave or distinct light emitting diodes to indicate which enclave is active, since the number of enclaves required may be large and not known in advance.)
8. Any hypervisor system must protect all security critical hardware and software from tampering, as described in Section 4.2.4.
9. In the case where a hypervisor is in use, the user could have complete freedom to choose the operating system on the personal enclave while the operating system on the professional enclave(s) could be chosen to match the Commonwealth's ICT policies (e.g. Windows Mobile). The NSA's specification for a secure enterprise mobility architecture [107] could also be a useful guide for selecting this operating system and configuring or modifying it to improve its security capabilities. (Note that the NSA specification does not cover hypervisor systems, but instead assumes that the device has just one operating system installed that is in complete control of the phone at all times. It is the author's opinion that this paradigm is too limiting, in that it prevents users from having a separate personal space on the phone or from accessing professional content at more than one security level. Nevertheless, even with a hypervisor system, much of the NSA's advice is applicable within each professional enclave.)
10. If the ability to handle data at different security classifications is desired, then it may be necessary to include more than one professional enclave. For example, a user who needs to connect to an unclassified corporate network and a restricted government network would need a personal enclave, professional (unclassified) enclave and professional (restricted) enclave. In some cases, many such separate enclaves may be required, including separate enclaves at the same level in order to accommodate compartments and caveats. It is possible for different level enclaves to use different operating systems or different security configurations if this assists with providing sufficient security for high classification levels, whilst allowing more functionality at lower levels.
11. In order to avoid attacks based on vulnerabilities in GSM, it may be necessary to disable GSM entirely on the smartphone, e.g. by modifying the operating system installed on each professional enclave to insist on a UMTS connection. More research should be done to determine if this is really necessary and if so, how it could best be achieved.

12. For the sake of risk limitation, it may be wise to disable some of the extra communication protocols available on smartphones, such as WiFi, Bluetooth and NFC. These protocols are not necessary for the smartphone's core functions of voice, text messages and Internet browsing, or for many available applications. Supporting these protocols adds unnecessary risk, especially for the highly insecure Bluetooth and relatively immature NFC. Note that Bluetooth is explicitly prohibited under current ICT policies for mobile devices handling information classified CONFIDENTIAL or higher ([110], Control 0682, p. 270) and is specifically mentioned by the NSA as a cause of concern ([107], p. 11). Whether this policy should be applied to the whole device or merely to the professional enclaves is debatable.

13. As per existing regulations ([110], Control 0687, p. 269), smartphones should not be allowed to process or store TOP SECRET information without DSD authorisation. This is because a smartphone could end up in the hands of an adversary, and any encryption used to protect the information stored on it could eventually be broken.

14. Intelligence belonging to Australia's allies should not be allowed on smartphones, regardless of classification, unless the nation concerned is satisfied with the security arrangements that are in place and has explicitly granted permission for this to occur, either through a general agreement or on a case-by-case basis.

15. The enclave separation should extend to billing, although this would require some modification of the software. Such modifications should not be made to the hypervisor itself, as this would entail re-accreditation, and should not involve the personal enclave, as this is untrusted and outside of the control of the organisation. The best solution would be to install call, text and data monitoring software within the corporate enclave(s), in order to meter professional usage separately. Personal usage could be calculated as the difference between the usage data on the service provider's bill and the professional usage.

16. The user should be free to choose his/her own service provider, with the bills paid by the user and reimbursement available for professional usage.

17. If separate personal and professional billing cannot be made available then the Commonwealth must be responsible for selecting the service provider and paying the bills, while the user must abide by a clearly defined policy for the extent of acceptable personal use (e.g. setting a maximum bill size that the Commonwealth is prepared to pay, requiring users to log and reimburse the Commonwealth for personal use, or whatever is deemed appropriate) .

18. On a device with separate professional and personal domains, the user is to have administrative rights in the personal domain only.

19. On a device with separate professional and personal domains, the Commonwealth is considered to own all information on the professional domain(s). The user retains ownership of the information on the personal domain. In the event that the device needs to be returned to the Commonwealth for upgrade, sanitisation of sensitive data or because the employee is leaving, the user is to be given a reasonable amount of time to extract the personal information first (subject to national security requirements). If this is not possible, for example because the

employee is under suspicion of involvement in a security breach, then the personal information is to be extracted by appropriately cleared personnel (with the necessary warrants) and returned to the user only after it has been checked and sanitised.

20. Existing ICT policies ([110], pp. 274-276) governing the public or out-of-office use of mobile devices must apply when using any professional enclave, regardless of its security classification. In particular, privacy filters should be used on the device's screen and "agencies should ensure personnel are aware not to access or communicate sensitive or classified information in public locations … unless extra care is taken to reduce the chance of being overheard or having the screen of the device observed" ([110], Control 0866, p. 274). To this end, employees should not use classified enclaves in public locations and should exercise extreme caution when using them in private locations that are outside of the user's control and thus may contain covert cameras, such as hotel rooms in foreign countries. If appropriately certified private input / output systems for smartphones are eventually developed (see Sections 6.2.2 and 6.2.3), then private usage could be ensured by mandating its use in all out-of-office situations (as an alternative to the existing measures).

21. ICT policies governing the use of smartphones in public or out-of-office should not apply when only the personal enclave is in use; this is consistent with the existing ICT policies as it is a special case of a device "with multiple operating states" ([110], p. 268).

22. A detailed policy should be developed to determine how (or if) government smartphones may be used in foreign countries with whom Australia does not have intelligence sharing agreements. Existing policy would suggest that this is allowed ([110], p. 275); however, only a few regulations and suggestions for doing so are provided. There is also scope for further research and development here, for example to provide a fast and covert means of wiping the contents of the device in the event that a government employee is compelled by foreign authorities to reveal the passwords needed to decrypt the various enclaves. For example, the smartphone could be programmed to wipe the contents of all enclaves if a special panic password is entered.

23. Any data transmission to or from corporate/government networks is to be encrypted using virtual private network software or similar. This is in agreement with the advice from the NSA [107]. Digital certificates are to be used for authentication of both the smartphone's professional enclave and the network it connects to, signed by a local certificate authority run by the organisation. (Note: The public key for the certificate authority would need to be stored on the smartphone's professional enclave in order to verify the network's certificate. An attacker who could change the local copy of this public key would be able to bypass the authentication of the network to the smartphone. However, the storage of the public key in an encrypted file system makes any meaningful modification of it impossible without knowledge of the user's login password.)

24. The information stored on any professional enclaves of the smartphone is to be encrypted, preferably with file system level encryption such as eCryptfs [127]. In

that case a lost or stolen smartphone does not pose as significant a security risk, in that there is a reasonable chance that the loss will be reported and the corporate enclave wiped remotely before the encryption can be broken. In order to facilitate regular changes to the enclave login password, the file system encryption system should use the password to encrypt a key stored in a separate area of the storage device, with the key used to encrypt the file system data. That way, changing the login password requires decrypting the key with the old password and re-encrypting it with the new password, rather than having to decrypt and re-encrypt the entire file system.

25. While the above policy of using file system encryption and remote wiping provides an extra layer of defence against the theft of sensitive data, this cannot be relied on completely. Stealing data is still possible if a stolen mobile device is immediately disabled to prevent remote wiping, and then transferred to a location in which external signals are blocked so that brute force computation can be used to break the encryption. This vulnerability is equivalent to that of sensitive data transmitted over the public Internet using a VPN, since in that case an eavesdropper could buffer encrypted VPN traffic for later cryptographic analysis. In either case, the attack would take a long time and be very computationally expensive, which means allowing data classified SECRET or lower to be exposed in this way is probably an acceptable risk.

26. Based on presently available technology, Commonwealth owned mobile devices must remain banned from secure areas of government buildings, especially if the device contains a personal domain that is administered by the user and could therefore be compromised when in that mode. It may be necessary to make some special exceptions to this rule, however, to allow for the situation when a smartphone's professional enclave needs to have new applications installed on it by IT staff. It is also possible that future smartphones could be developed which are able to be put into a special operation mode that makes them safe for use inside secure areas; this is discussed in more detail in Section 6.2.1.

27. In order to safeguard the reputation of the Commonwealth, the provisions for acceptable use of information and communications technology should apply to both professional and personal domains on the device, as regards offensive material etc. However, ICT policies such as banning the use of services such as Gmail and rules for software installation should not apply to the personal domain.

28. It may be necessary to enforce stricter password policies than those that are used by default on the chosen model of smartphone, in order to meet the requirements of the Commonwealth's ICT policies. Preferably, such policies should be enforced in software rather than relying on user compliance, which is possible if an open source operating system were used and may not be possible on some closed source operating systems.

29. The passwords used to unlock the different enclaves must all be different, and not related to each other in any obvious way. In particular, the password (if any) used on the personal enclave must be different to the passwords used on the professional enclaves. The passwords should also differ from passwords used to access government networks, even for enclaves and networks at the same level.

This is an important damage limitation measure for the situation when a captured mobile phone is compromised, so that even an adversary with knowledge of all mobile device passwords cannot use these to gain unauthorised access to government networks. As this cannot be enforced in software when using a hypervisor system, users must be briefed on this matter and agree to this condition prior to being allowed use of a mobile device for professional purposes.

30. All the enclave passwords (except the password used for accessing the personal enclave) are to be recorded and stored as classified material, with the classification being the greater of UNCLASSIFIED FOR-OFFICIAL-USE-ONLY and the classification of the enclave it provides access to. Note that the existing practice of never recording network passwords cannot be applied, as it is not possible to reset a password for an encrypted file system without destroying the contents of that file system.
31. Facial recognition is not to be used as the sole authentication mechanism on any enclave storing government information, but may be used as a second factor of authentication. Users should be free to choose their own authentication method on the personal enclave, however.
32. The gathering of quality of service metrics from any government enclave must be disabled, and ideally this should be disabled for the entire device.

6.2 Recommendations for Further Research

The author recommends further research in the following areas.

6.2.1 Secure Area Special Operation Mode for Smartphones

One useful extension to smartphones featuring securely separated security domains (e.g. personal, UNCLASSIFIED professional, RESTRICTED professional, etc) would be the ability to switch the device into a mode that makes it safe to use in secure government areas. This would involve disabling the personal enclave from being foregrounded, in order to prevent untrusted code on this enclave from controlling the phone's input devices and thus leaking sensitive information to the personal enclave from the physical environment. (The hypervisor can be trusted to prevent data leaking to the personal enclave from professional enclaves.) It may also be considered necessary to disable some risky hardware altogether while in the secure area mode, for instance cameras, Bluetooth and WiFi. Obviously, the hardware and software used by the user to switch into the secure area mode would need to be a trusted part of the hypervisor system, as the system used for switching between the different enclaves is.

6.2.2 Private Input / Output Devices

There is scope for further research and development towards making smartphones more secure for use in public, for example by developing software to allow a smartphone to use a plug-in head-mounted audiovisual display (with hand, head and / or eye tracking) instead of a touchscreen. (Note that various types of head-mounted display devices already exist, such as the Z800 3DVisor [128], as well as others in development, such as Google's Project Glass [129]. These are not developed with security in mind, however, so there is significant scope for further research here.) Ideally, secure input should be based on detecting hand movements with respect to a virtual keyboard projected as a three dimensional image, with the keyboard layout randomised after every keystroke to prevent eavesdropping attacks based on letter frequency analysis. The cameras used for capturing the hand movements could also capture the natural visual scene for the purpose of providing that to the user with the content information overlaid. Such a system should be adequately secured from data leakage (e.g. by transmitting information between the smartphone and headset in encrypted form) and use mutual authentication between the headset and smartphone (to avoid a device substitution attack).

6.2.3 TRIODE

A possible extension of the above concept is to create a trusted input / output device that plugs into an untrusted COTS smartphone's USB port. The TRusted Input Output DEvice (TRIODE) could consist of a head-mounted audiovisual display (for private sound and vision output) and hand/eye tracking input device (for pointer control and private input on a dynamically randomised keyboard), which are connected to a small controller box containing an embedded microcontroller. (A conventional keypad and microphone could also be connected, although they could not be used for inputting classified information in public.) The TRIODE controller could set up a network connection to the smartphone over wi-fi or Bluetooth, which if necessary is managed by a custom application running on the smartphone. Then the TRIODE controller could set up a VPN connection to a sensitive government network through the smartphone and the carrier's 3G service (or even through WiFi if this service is available).

In order to limit the risks from using uncertified COTS hardware, both the smartphone and the carrier's 3G network must be considered to be untrusted; in fact, the smartphone can be considered to be simply an extension of the untrusted channel over the open Internet. In addition, the wireless link between the TRIODE and the smartphone is untrusted. Since the TRIODE (rather than the smartphone) must authenticate the user to the sensitive network, this would require the user to input his / her password for the sensitive network using the TRIODE not the smartphone. It would also be necessary for the sensitive network to authenticate the TRIODE, so that it can be certain that it is communicating with trusted hardware and not simply an emulator application run on the smartphone by a user who does not like carrying the TRIODE hardware. Likewise, the TRIODE would also need to authenticate the sensitive network using a digital certificate, with the public key required for verifying it stored on the TRIODE in a tamper resistant and tamper evident chip.

As a trusted device, the TRIODE would need to lock automatically after a short period of non-use, with a password required to unlock it. The unlock password would be stored on the TRIODE only as a salted hash. It may also be necessary to drop all open VPN connections after an extended period of non-use, so that the user would need to re-establish those after unlocking the TRIODE.

The computational load on the TRIODE could be reduced by performing as much processing as possible on the remote server on the sensitive network, which ideally would contain all the secure applications that are accessed using TRIODE as well as providing permanent storage of the data they operate on. In other words, the TRIODE would act as a kind of mobile trusted thin client. (This approach is consistent with the concept of a Defence Data Centre with centralised processing, part of the Defence ICT Mobility vision. See [126], p. 10.) This reduces the risks associated with storing sensitive material on a mobile device, since the design limits the amount of sensitive information that is permanently stored on the TRIODE in either plaintext or encrypted form. Plaintext sensitive information is never revealed to the untrusted smartphone at all. However, if performance constraints demand it, the TRIODE could make use of the untrusted smartphone’s storage capability, by sending it encrypted data to store, with the symmetric encryption key remaining on the TRIODE, along with a hash to ensure integrity. Storing encrypted data on the smartphone is not dangerous, as the key needed for decrypting it is never stored on or processed by the smartphone itself. Ideally, the key should not be stored in plaintext even on the TRIODE, but rather should be encrypted using a password known only to the user and not stored on the TRIODE, except possibly as a salted hash.

It must be recognised that, whether or not the TRIODE makes explicit use of the smartphone for storing encrypted data, there could be encrypted data stored on the smartphone at any time. This is because the operating system on the smartphone is untrusted, and therefore no assumptions can be made that the smartphone will discard the encrypted information it receives after forwarding it. Therefore, the use of the TRIODE would require a slight change to the policy in the Australian Government information security manual ([110], p. 269), so that classified information may be stored on a privately owned mobile device if it is encrypted with a key that is never revealed to the device, rather than the present policy of prohibiting classified storage entirely. Such a policy change does not represent a significant increase in risk, since existing VPN technologies (as well as the TRIODE) transmit classified data in encrypted form over the public Internet, and there are no means for preventing this encrypted data from being intercepted and stored by adversaries whilst in transit.

As a further extension, the TRIODE could allow the user to change between a number of different sensitive networks at different classifications, perhaps using an MLS hypervisor system such as the Green Hills INTEGRITY Separation Kernel. Fresh authentication credentials would need to be provided by the user when first connecting to a sensitive network and when switching to it after a long hiatus. Alternatively, the TRIODE could function at a single level at a time, with MLS access to different sensitive networks managed on the server side. In that case, the TRIODE device would need to have a certified feature for erasing all content information stored on it before switching levels (and also when dropping VPN connections after a long period of disuse), without destroying important non-content information such as the operating system. One way to achieve this would be to store the TRIODE software in write-protected memory, with sensitive information obtained over the VPN connection stored in volatile memory. The erase operation would need to use hardware circuitry to overwrite the volatile memory several times with random data, before rebooting the operating system; a new VPN connection could then be established by the user at the new level.

The key advantage of a TRIODE would be that, once the device was certified, it could be used for accessing sensitive information from a variety of COTS smartphones that have not been certified, even smartphones that are owned and poorly administered by naïve users and which are infected by malware. Deploying the TRIODE on new smartphone models would be fairly simple, as this would involve writing a small smartphone application to manage the USB virtual network interface, at the very most, and this application would not need to be trusted either. Since the TRIODE itself would be designed to act as a thin client, it would be very easy to upgrade or extend the suite of applications provided by the sensitive network server, without needing to modify the hardware or software on the TRIODE or needing to reaccredit it. This means that, subject to careful monitoring for security holes and design flaws, the TRIODE could conceivably have a useful lifetime that is many times greater that of any COTS smartphone, potentially saving money that would have had to be spent accrediting a large number of smartphone models.

It is the author's belief that a system along the same lines as TRIODE would be a significantly better solution to the issues raised in this report than the recommendation to use the Green Hills Platform for Trusted Mobile Devices, since the TRIODE would allow for private usage in an untrusted physical environment whereas a smartphone on its own does not. In addition, the use of a hypervisor based system forces users to adopt a particular model of smartphone hardware, hence preventing the use of popular models such as iPhones; the TRIODE, in contrast, would allow users to access sensitive material in a secure manner through a wide variety of smartphones.

The TRIODE also offers significant advantages over the use of distinct personal and professional phones. For instance, the TRIODE would allow access to any number of different security domains using just the user's smartphone and the TRIODE, whereas the multi-phone solution would require as many different phones as there were security domains. The solution of distinct personal and professional phones could allow access to multiple security domains using just two phones, if the professional phone was a multi-enclave hypervisor system, but even then the maximum number of domains that could be supported would be limited by the amount of available data storage space. When using the TRIODE this would be less of an issue, as the data for the different domains would be stored on a server rather than on the device. Moreover, the multi-phone solution would not allow private usage in an untrusted physical environment.

The TRIODE has some features in common with the Digital Video Guard (DVG) and associated USB guard, developed by DSTO [130]. These allow the creation of a secure channel between a remote server and the input and output devices of an untrusted desktop computer. The DVG is designed to be inserted into the Digital Visual Interface (DVI) data connection between the computer and its monitor, allowing an encrypted video signal to be decrypted prior to display on the monitor. Likewise, the USB guard separates the USB input devices such as the mouse and keyboard from the computer, allowing the input data to be encrypted prior to its receipt by the computer. Since the DVG and USB guard are designed to be inserted into the data connections between a computer and its peripherals, this presents a serious challenge to their use in mobile devices, where the computer and its peripherals are integrated into one unit. This could be overcome if a device is manufactured that includes its own touch screen display and keyboard, together with the encryption and decryption capabilities of the USB guard and DVG, which may then be connected to an untrusted smartphone by a wired or wireless link. However such a device would in effect be a TRIODE, albeit without the capability for private use in an untrusted physical environment.

Despite its advantages, it is clear that a significant amount of research and development would need to be done before the TRIODE became a viable option for operational policy. In the meantime, the recommendations in Section 6.1 stand.

6.2.4 Side Channels

Further research needs to be done into the issue of side channels. Before any specific smartphone or associated hardware is approved for Australian Government use, the electromagnetic radiation that it emits must be analysed along the same lines as [45]. It is not acceptable for there to be any measurable correlation between the electromagnetic emission signal and any encryption key material or plaintext data on the device. Power analysis side channels are of secondary concern, since this depends on an adversary obtaining custody of the device. However, it must not be possible for power analysis to be used to circumvent a smartphone's password or extract other useful information from a locked phone.

Further, if a smartphone with separate enclaves is used (as recommended in Section 6.1), then the possibility of any covert channel between enclaves must be eliminated. For example, it must not be possible to leak information using cache based or timing attacks, as discussed in Sections 2.9 and 4.1.3. While this should be covered by the hypervisor certification, there may still be value in conducting further research to provide an independent confirmation of this.

7. Conclusion

There are many issues and risks associated with the use of smartphones for professional purposes, especially regarding security. Taking these into consideration, it seems that the present policy of certifying specific COTS smartphones for connecting to sensitive government networks, including devices not owned by the government agency, is wasteful and introduces unnecessary security risks. Based on the technologies that are currently available, a far more effective strategy would be to certify just a small number of smartphones which provide separation between several different security domains (such as the Green Hills Platform for Trusted Mobile Devices). This would allow the devices to connect to a range of government networks at different classification levels as well as keeping personal use separate. Such separation is either not available on the devices currently certified by DSD or is not a DSD certified feature on those devices. Most importantly, the trusted separation approach on a smartphone owned by the government agency would allow the agency's ICT staff to retain full control of the enclaves used for handling sensitive data, while allowing the employee to retain full control of the enclaves for personal use. Looking further ahead, an even more flexible solution would be to allow the use of privately owned smartphones of any variety, but only as untrusted devices that form part of a VPN link between special trusted thin-client hardware (TRIODE) and a cloud server on a sensitive government network. Such an approach would require extensive research and development before it could be considered by policymakers, however.

References

1. Timson, L. *Use a smartphone? You may want to read this*. 2012 Retrieved 2/3/2012]; Available from: http://www.theage.com.au/it-pro/security-it/use-a-smartphone-you-may-want-to-read-this-20120301-1u4jh.html.

2. Emspak, J. *7 Security Tips for Smartphone Users*. 2011 Retrieved 29/2/2012]; Available from: http://www.securitynewsdaily.com/1053-security-tips-smartphones.html.

3. McMillan, R. *Android Security Chief: Mobile-phone Attacks Coming*. 2009 Retrieved 29/2/2012]; Available from: http://www.pcworld.com/businesscenter/article/170092/android_security_chief_mobilephone_attacks_coming.html.

4. Kendrick, J. *Latest smartphone market share numbers: Apple is flat, Google going strong*. 2011 Retrieved 29/2/2012]; Available from: http://www.zdnet.com/blog/mobile-news/latest-smartphone-market-share-numbers-apple-is-flat-google-going-strong/2387.

5. Schroeder, S. *Honeycomb Brings Data Encryption to Android Tablets*. Mashable Tech 2011 Retrieved 29/2/2012]; Available from: http://mashable.com/2011/02/03/android-3-0-encryption/.

6. Radia, R. *Why you should always encrypt your smartphone*. 2011 Retrieved 29/2/2012]; Available from: http://arstechnica.com/gadgets/guides/2011/01/why-you-should-always-encrypt-your-smartphone.ars/2.

7. *Notes on the implementation of encryption in Android 3.0*. 2011 Retrieved 29/2/2012]; Available from: http://source.android.com/tech/encryption/android_crypto_implementation.html.

8. Lendino, J. *Kill Your Phone Remotely*. 2009 Retrieved 29/2/2012]; Available from: http://www.pcmag.com/article2/0,2817,2352755,00.asp.

9. *iOS Hardening Configuration Guide - FOR iPOD TOUCH, iPHONE AND iPAD RUNNING iOS 5.1 OR HIGHER*. 2012 Retrieved 30/3/2012]; Available from: http://www.dsd.gov.au/publications/iOS5_Hardening_Guide.pdf.

10. *iOS: Understanding passcodes*. 2012 Retrieved 15/3/2012]; Available from: http://support.apple.com/kb/HT4113.

11. *iOS: Wrong passcode results in red disabled screen*. 2012 Retrieved 15/3/2012]; Available from: http://support.apple.com/kb/ht1212.

12. Schramm, M. *Most common iOS passcodes discovered by developer*. 2011 Retrieved 15/3/2012]; Available from: http://www.tuaw.com/2011/06/14/most-common-ios-passcodes-discovered-by-developer/.

13. *iOS Configuration Profile Reference*. 2011 Retrieved 15/3/2012]; Available from: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/iPhoneConfigurationProfileRef.pdf.

14. Timson, L. *iPhone 4S security hole uncovered*. 2011 Retrieved 15/3/2012]; Available from: http://www.theage.com.au/it-pro/security-it/iphone-4s-security-hole-uncovered-20111019-1m6xt.html.
15. *How Do Authentication and Key generation work in a GSM network?* . 2010 Retrieved 21/5/2012]; Available from: http://www.gsm-security.net/faq/gsm-authentication-key-generation.shtml.
16. *Specifications - Confidentiality Algorithms*. 2012 Retrieved 1/3/2012]; Available from: http://www.3gpp.org/Confidentiality-Algorithms.
17. Sidhardhan, S. *Sim Cloning*. 2011 Retrieved 1/3/2012]; Available from: http://www.5ne.org/sim-cloning/.
18. *How to Clone a SIM Card*. 2012 Retrieved 21/5/2012]; Available from: http://www.ehow.com/how_4770451_clone-sim-card.html.
19. *How to Clone Your Cell Phone's SIM Card (maybe)*. 2008 Retrieved 1/3/2012]; Available from: http://www.techtraction.com/2008/10/01/how-to-clone-your-cell-phones-sim-card-maybe/.
20. *Why You Cannot Clone a SIM Chip*. 2009 Retrieved 1/3/2012]; Available from: http://www.techtraction.com/2009/01/19/why-you-cannot-clone-a-sim-chip/.
21. *Mobile buyers beware, say police*. 2010 Retrieved 4/5/2012]; Available from: http://www.amta.org.au/articles/Mobile.buyers.beware.say.police.
22. *FAQs on mobile security*. 2012 Retreived 5/4/2012]; Available from: http://www.amta.org.au/pages/amta/FAQs.on.mobile.security.
23. Meyer, U. and S. Wetzel, *A Man-in-the-Middle Attack on UMTS*, in *ACM Workshop on Wireless Security*. 2004: Philadelphia.
24. Niemi, A., J. Arkko, and V. Torvinen. *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*. RFC 3310 2002 Retrieved 2/3/2012]; Available from: http://tools.ietf.org/html/rfc3310.
25. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification*. 2011 Retrieved 6/3/2012]; Release 10:[Available from: http://www.3gpp.org/ftp/Specs/archive/35_series/35.201/35201-a00.zip.
26. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; General Report on the Design, Speification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms*. 2001 Retrieved 6/3/2012]; Release 4:[Available from: http://www.3gpp.org/ftp/Specs/archive/33_series/33.908/33908-400.zip.
27. Geiger, H. *NFC Phones Raise Opportunities, Privacy And Security Issues*. 2011 Retrieved 2/3/2012]; Available from: https://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues.
28. ISO/IEC-18092, *Information technology - Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*. 2004.

29. ISO/IEC-21481, *Information technology - Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol-2 (NFCIP-2)*. 2004.

30. ISO/IEC-13157-1, *Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 1: NFC-SEC NFCIP-1 security services and protocol* 2010.

31. ISO/IEC-13157-2, *Information technology -- Telecommunications and information exchange between systems -- NFC Security -- -- Part 2: NFC-SEC cryptography standard using ECDH and AES*. 2010.

32. *Standard ECMA-386 - NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES*. 2010 Retrieved 4/5/2012]; Available from: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-386.pdf.

33. *Standard ECMA-385 - NFC-SEC: NFCIP-1 Security Services and Protocol* 2010 Retrieved 4/5/2012]; Available from: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-386.pdf.

34. Meindl, R. *NFCIP-1 Security Standard Protects Near Field Communication*. 2009 Retrieved 5/4/2012]; Available from: http://docbox.etsi.org/workshop/2009/200901_SECURITYWORKSHOP/NXP_MEINDL_NFCIP1SecurityStandardProtectsNearFieldCommunication.pdf.

35. Haselsteiner, E. and K. Breitfuß, *Security in Near Field Communication (NFC) - Strengths and Weaknesses*, in *RFID Security 06*. 2006, Philips Semiconductors: Graz.

36. Padgette, J., K. Scarfone, and L. Chen. *Guide to Bluetooth Security*. 2012 Retrieved 11/10/2012]; Available from: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf.

37. *iOS Hardening Configuration Guide - FOR iPOD TOUCH, iPHONE AND iPAD RUNNING iOS 4.3.3 OR HIGHER*. 2011 Retrieved 30/3/2012]; Available from: http://www.dsd.gov.au/publications/iOS_Hardening_Guide.pdf.

38. *DoD Bluetooth Peripheral Device Security Requirements*. 2010 Retrieved 30/3/2012]; Available from: http://iase.disa.mil/stigs/downloads/pdf/dod_bluetooth_requirements_spec_20100716.pdf.

39. Fleishman, G. *Battered, but not broken: understanding the WPA crack*. 2008 Retrieved 2/3/2012]; Available from: http://arstechnica.com/security/news/2008/11/wpa-cracked.ars/1.

40. Viehböck, S. *Brute forcing Wi-Fi Protected Setup - When poor design meets poor implementation*. 2011 Retrieved 2/3/2012]; Available from: http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

41. *Seamless and Secure Mobility*. 2011 Retrieved 7/3/2012]; Available from: http://www.nist.gov/itl/antd/emntg/ssm_seamlessandsecure.cfm.

42. Melia, T., et al. *IEEE 802.21 Mobility Services Framework Design (MSFD)*. 2009 Retrieved 7/3/2012]; RFC 5677:[Available from: http://www.rfc-editor.org/rfc/rfc5677.txt.

43. *TEMPEST FUNDAMENTALS*. 1982 Retrieved 30/3/2012]; Available from: http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm.

44. Simonite, T. *Eavesdropping Antennas Can Steal Your Smart Phone's Secrets*. Technology Review 2012 Retrieved 16/3/2012]; Available from: http://www.technologyreview.com/communications/39855/page1/.

45. Jun, B. and G. Kenworthy. *Is Your Mobile Device Radiating Keys?* RSA Conference 2012 2/3/2012; Available from: http://www.cryptography.com/public/pdf/2012-Jun-Kenworthy-MobileDeviceLeakage.pdf.

46. Kocher, P.C., J.M. Jaffe, and B.C. Jun, *Differential Power Analysis*. 2009, Cryptography Research Inc.: US Patent No. 7634083 B2.

47. Kocher, P.C. *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. 1999 Retrieved 16/5/2012]; Available from: http://www.cryptography.com/public/pdf/TimingAttacks.pdf.

48. Brumley, D. and D. Boneh. *Remote Timing Attacks are Practical*. 2003 Retrieved 17/5/2012]; Available from: http://crypto.stanford.edu/~dabo/abstracts/ssl-timing.html.

49. Aumuller, C., et al. *Fault attacks on RSA with CRT: Concrete Results and Practical Countermeasures*. 2002 Retrieved 17/5/2012]; Available from: http://eprint.iacr.org/2002/073.pdf.

50. Pellegrini, A., V. Bertacco, and T. Austin. *Fault-Based Attack of RSA Authentication*. 2010 Retrieved 17/5/2012]; Available from: www.merit.edu/events/mmc/pdf/2010_pellegrini.pdf.

51. Wang, Z. and R.B. Lee. *Covert and Side Channels due to Processor Architecture*. 2006 Retrieved 17/5/2012]; Available from: http://palms.ee.princeton.edu/PALMSopen/wang06covert.pdf.

52. *Common Criteria Evaluation and Validation Scheme - Validation Report - Green Hills Software - IN-ICR750-0402-GH01_Rel INTEGRITY-178B Separation Kernel*. 2011 Retrieved 16/2/2012]; Available from: http://www.commoncriteriaportal.org/files/epfiles/st_vid10362-vr.pdf.

53. Lemos, R. *Apple iOS: Why it's the most secure OS, period*. 2011 Retrieved 19/3/2012]; Available from: http://www.infoworld.com/print/162792.

54. *Hacker reveals iOS malware vulnerability, gets punished*. 2011 Retrieved 20/3/2012]; Available from: http://www.gmanetwork.com/news/story/238101/scitech/hacker-reveals-ios-malware-vulnerability-gets-punished.

55. Lincoln, R.A. *iOS Bug Allows Malware to Be Sold in Apple App Store*. 2011 Retrieved 20/3/2012]; Available from: http://www.tomsguide.com/us/iOS-Apple-iPad-iPhone-malware,news-13122.html.

56. Moses, A. *Malicious copycat iPhone virus unleashed*. 2009 Retrieved 20/3/2012]; Available from: http://www.theage.com.au/digital-life/iphone/malicious-copycat-iphone-virus-unleashed-20091124-je7t.html.

57. Grubb, B. '*Charlatans and scammers': Googler slams security software firms*. 2011 Retrieved 20/3/2012]; Available from:

http://www.theage.com.au/technology/security/charlatans-and-scammers-googler-slams-security-software-firms-20111123-1ntpu.html.

58. Frier, S. *Google Android malware surges 472 per cent* 2011 Retrieved 19/3/2012]; Available from: http://www.theage.com.au/digital-life/mobiles/google-android-malware-surges-472-per-cent-20111116-1nhw2.html.

59. Finkle, J. *More insecure Google Android apps uncovered: security experts*. 2011 Retrieved 19/3/2012]; Available from: http://www.theage.com.au/technology/security/more-insecure-google-android-apps-uncovered-security-experts-20110815-1itj6.html.

60. *Android Security Overview*. 2012 Retrieved 19/3/2012]; Available from: http://source.android.com/tech/security/index.html.

61. *iOS Security*. 2012 Retrieved 25/6/2012]; Available from: http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf.

62. Felt, A.P., et al., *Android Permissions Demystified*, in *ACM Conference on Computer and Communications Security* 2011: Chicago.

63. Jeon, J., et al. *Dr. Android and Mr. Hide: Fine-grained security policies on unmodified Android*. 2011 Retrieved 19/3/2012]; Available from: http://www.cs.umd.edu/~jfoster/papers/acplib.pdf.

64. Svajcer, V. *Android malware spies on your SMS messages - but is it part of the Zeus family?* 2011 Retrieved 19/3/2012]; Available from: http://nakedsecurity.sophos.com/2011/07/09/android-malware-spies-sms-messages-zeus-family/.

65. Castillo, C. *Dissecting Zeus for Android (or Is It Just SMS Spyware?)*. 2011 Retrieved 19/3/2012]; Available from: http://blogs.mcafee.com/mcafee-labs/dissecting-zeus-for-android-or-is-it-just-an-sms-spyware.

66. Apvrille, A. and K. Yang. *Defeating mTANs for profit*. 2011 Retrieved 15/1/2013]; Available from: http://www.fortiguard.com/sites/default/files/shmoocon2011_zitmo-slides.pdf.

67. Eckhart, T. *CarrierIQ*. 2011 Retrieved 8/3/2012]; Available from: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.

68. Roskowski, S., et al., *Data collection associated with components and services of a wireless communication network*. 2011, CARRIER IQ, INC.: USA.

69. Billard, A., S. Chenoweth, and C. Owen, *Considerations for Realising the Future Defence Architecture for MLS Access*. 2012, Defence Science and Technology Organisation.

70. Griffin, M. *Office gadgets casting a pall of 'time pollution'*. 2011 19/11/2011 23/1/2012]; Available from: http://www.theage.com.au/technology/technology-news/office-gadgets-casting-a-pall-of-time-pollution-20111118-1nni8.html.

71. Gruman, G. *Lost in BYOD's uncharted legal waters*. 2012 Retrieved 14/3/2012]; Available from: http://www.infoworld.com/t/byod/lost-in-byods-uncharted-legal-waters-180793.

72. Tindal, S. *IT just like Alice in Wonderland: Defence*. 2012 Retrieved 27/3/2012]; Available from: http://www.zdnet.com.au/it-just-like-alice-in-wonderland-defence-339334268.htm.

73. Rodriguez, A. *Protect Your Android Phone With Security Apps*. 2010 Retrieved 19/3/2012]; Available from: http://www.pcworld.com/article/212192/protect_your_android_phone_with_security_apps.html.

74. German, K. *Sprint offers McAfee security apps for Android*. 2011 Retrieved 19/3/2012]; Available from: http://reviews.cnet.com/8301-19736_7-20090804-251/sprint-offers-mcafee-security-apps-for-android/.

75. Rashid, F.Y. *IT Security & Network Security News & Reviews: 10 iOS Security Apps to Protect Your iPhone, iPad from Hackers*. 2011 Retrieved 20/3/2012]; Available from: http://www.eweek.com/c/a/Security/10-iOS-Security-Apps-to-Protect-Your-iPhone-iPad-from-Hackers-492794/.

76. Lai, R. *Andy Rubin: Ice Cream Sandwich's Face Unlock is developed by PittPatt*. 2011 Retrieved 20/3/2012]; Available from: http://www.engadget.com/2011/10/19/andy-rubin-ice-cream-sandwichs-face-unlock-is-developed-by-pit/.

77. Murphy, D. *Blogger Breaks Android Face Recognition with... a Picture?* 2011 Retrieved 20/3/2012]; Available from: http://www.pcmag.com/article2/0,2817,2396321,00.asp.

78. Brian, M. *Can Android's new 'Face Unlock' feature be hacked using a photo? Google says no.* 2011 Retrieved 20/3/2012]; Available from: http://thenextweb.com/google/2011/10/20/can-androids-new-face-unlock-feature-be-hacked-using-a-photo-google-says-no/.

79. D'Orazio, D. *Android 4.1 Jelly Bean 'Liveness Check' hopes to stop Face Unlock from being fooled by photos*. 2012 Retrieved 15/1/2013]; Available from: http://www.theverge.com/2012/6/30/3128657/android-4-1-jelly-bean-liveness-check-face-unlock.

80. Morris, P. *Android Jelly Bean's Facial Liveness Check Can Be Bypassed Using Simple Image Manipulation*. 2012 Retrieved 15/1/2013]; Available from: http://www.redmondpie.com/android-jelly-bean-facial-liveness-check-can-be-bypassed-using-simple-image-manipulation-video/.

81. Topolsky, J. *Motorola Atrix 4G review*. 2011 Retrieved 7/5/2012]; Available from: http://www.engadget.com/motorola/atrix-4g-review/.

82. Matsumoto, T., et al. *Impact of Artificial "Gummy" Fingers on Fingerprint Systems* in *Optical Security and Counterfeit Deterrence Techniques IV*. 2002: SPIE.

83. Mor, G. *Persay launched Voice Authentication for iPhone Apps*. 2010 Retrieved 7/5/2012]; Available from: http://www.thewadi.com/persay-launched-voice-authentication-for-iphone-apps/.

84. *Reduce Operational Costs and Fight Fraud with Secure Automated Speaker Verification*. 2012 Retrieved 7/5/2012]; Available from: http://www.nuance.com/for-business/by-

solution/customer-service-solutions/solutions-services/inbound-solutions/voice-authentication-biometrics/index.htm.

85. Talmor, E. *VoiceProof Online-Secure Transactions Solution*. 2009 Retrieved 7/5/2012]; Available from: www.sentry-com.net/files/VoiceProof_Online_Manual.pdf.

86. Lobkovsky, A. *Are Android unlock patterns as secure as numeric PINs?* 2010 Retrieved 8/5/2012]; Available from: http://playingwithmodels.wordpress.com/2010/04/14/andorid_unlock_patterns/.

87. Kocher, P.C., J.M. Jaffe, and B.C. Jun, *Cryptographic computation using masking to prevent differential power analysis and other attacks* 2010, Cryptography Research, Inc.: US.

88. Shamir, A., *Method and Apparatus for protecting public key schemes from timing and fault attacks*. 1999: U.S.A.

89. *Go Ahead - Bring Your Own Device to Work* 2011 Retrieved 15/2/2012]; Available from: http://www.att.com/gen/press-room?pid=21555&cdvn=news&newsarticleid=32980.

90. Simonite, T. *App Gives Android a Split Personality*. Technology Review 2011 Retrieved 15/2/2012]; Available from: http://www.technologyreview.com/computing/32445/.

91. *The Divide™ Platform*. 2012 Retrieved 15/2/2012]; Available from: http://www.divide.com/product.php.

92. Simonite, T. *One Smart Phone, Two Personalities*. Technology Review 2011 Retrieved 15/2/2012]; Available from: http://www.technologyreview.com/communications/38865/page1/.

93. *vLogix Mobile, First Mobile Virtualization Solution Ready for the Mass Market*. 2012 Retrieved 15/2/2012]; Available from: http://www.virtualization.net/3362-vlogix-mobile-first-mobile-virtualization-solution-ready-for-the-mass-market/.

94. *Mobile Virtualization: How it Works*. 2012 Retrieved 16/2/2012]; Available from: http://www.redbend.com/index.php?option=com_content&view=article&id=133%3Amobile-virtualization-how-it-works&catid=33&Itemid=61&lang=en.

95. *Mobile Virtualization*. 2012 Retrieved 16/2/2012]; Available from: http://www.redbend.com/index.php?option=com_content&view=article&id=134&Itemid=60&lang=en.

96. *VMware Horizon Mobile and VMware Mobile Virtualization Platform*. 2012 Retrieved 15/2/2012]; Available from: http://www.vmware.com/products/mobile/overview.html.

97. Gohring, N. *VMWare Shows off Mobile Virtualization on Android*. 2011 Retrieved 15/2/2012]; Available from: http://www.pcworld.com/article/219671/vmware_shows_off_mobile_virtualization_on_android.html.

98. *Green Hills Platform for Trusted Mobile Devices*. 2012 Retrieved 16/2/2012]; Available from: http://www.ghs.com/products/mobile_devices.html.

99. *Green Hills Software INTEGRITY-178B Separation Kernel Security Target Version 4.2*. 2010 Retrieved 16/2/2012]; Available from: http://www.commoncriteriaportal.org/files/epfiles/st_vid10362-st.pdf.

100. Ashkenazi, A. *Security Features in the i.MX31 and i.MX31L Multimedia Applications Processors*. 2005 Retrieved 5/6/2012]; Available from: http://www.freescale.com/files/32bit/doc/white_paper/IMX31SECURITYWP.pdf.

101. Hoover, J.N. *National Security Agency Plans Smartphone Adoption*. 2012 Retrieved 21/3/2012]; Available from: http://www.techweb.com/news/232600238/national-security-agency-plans-smartphone-adoption.html.

102. *L-3 Guardian*. 2008 Retrieved 21/3/2012]; Available from: http://www2.l-3com.com/cs-east/ia/smeped/ie_ia_smeped.shtml.

103. *Sectéra Edge (SME PED)*. 2012 Retrieved 21/3/2012]; Available from: http://www.gdc4s.com/content/detail.cfm?item=32640fd9-0213-4330-a742-55106fbaff32.

104. Kenyon, H. *First Android device certified for Pentagon personnel*. 2011 Retrieved 27/3/2012]; Available from: http://defensesystems.com/articles/2011/10/28/disa-approves-first-andriod-device-for-dod.aspx.

105. Ayers, J. *Dell Mobile Security for Android Officially Certified for Government Use by DISA*. 2011 Retrieved 27/3/2012]; Available from: http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2011/10/28/dell-mobile-security-for-android-officially-certified-for-government-use-by-disa.aspx.

106. Zakaria, T. *Not so simple: U.S. spy agency trying to go mobile*. 2011 Retrieved 21/3/2012]; Available from: http://www.reuters.com/article/2011/09/23/us-usa-intelligence-mobile-idUSTRE78M5BI20110923.

107. *Mobility Capability Package*. 2012 Retrieved 8/3/2012]; Available from: http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_(Version_1.1U).pdf.

108. Kenyon, H. *Army program for secure Android kernel technology gets attention of NSA and White House*. 2011 Retrieved 27/3/2012]; Available from: http://defensesystems.com/articles/2011/10/11/ausa-secure-andriod-kernel-technology.aspx.

109. *EPL - Evaluated Products List*. 2012 Retrieved 28/3/2012]; Available from: http://www.dsd.gov.au/infosec/epl/index.php.

110. *Australian Government Information Security Manual - Controls*. 2012 Retrieved 11/10/2012]; Available from: http://www.dsd.gov.au/publications/Information_Security_Manual_2012_Controls.pdf?&updatedSep12.

111. Schneier, B. *Should Enterprises Give In to IT Consumerization at the Expense of Security?* 2010 Retrieved 22/3/2012]; Available from: http://www.schneier.com/essay-323.html.

112. Pennington, S. *BlackBerry losing corporate popularity*. 2011 Retrieved 22/3/2012]; Available from: http://www.theage.com.au/it-pro/business-it/blackberry-losing-corporate-popularity-20111017-1lswi.html.

113. Turney, D. *BlackBerry tries to remain relevant*. 2012 Retrieved 22/3/2012]; Available from: http://www.theage.com.au/it-pro/business-it/blackberry-tries-to-remain-relevant-20120123-1qd6j.html.

114. Karena, C. *Laying down the BYO law*. 2012 Retrieved 22/3/2012]; Available from: http://www.theage.com.au/it-pro/business-it/laying-down-the-byo-law-20120320-1vgsz.html.

115. Timson, L. *Apple surfs into workplace on BYO wave*. 2011 Retrieved 23/3/2012]; Available from: http://www.theage.com.au/it-pro/business-it/apple-surfs-into-workplace-on-byo-wave-20110923-1ko2p.html.

116. Turney, D. *Are companies ready for Android?* 2012 Retrieved 23/3/2012]; Available from: http://www.theage.com.au/it-pro/business-it/are-companies-ready-for-android-20120110-1psmd.html.

117. *Special Publications (800 Series)*. 2012 Retrieved 29/3/2012]; Available from: http://csrc.nist.gov/publications/PubsSPs.html.

118. Jansen, W. and K. Scarfone. *Guidelines on Cell Phone and PDA Security*. 2008 Retrieved 29/3/2012]; Available from: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.

119. Frankel, S., et al. *Guide to IPsec VPNs*. 2005 Retrieved 29/3/2012]; Available from: http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.

120. *FIPS Publications*. 2012 Retrieved 29/3/2012]; Available from: http://csrc.nist.gov/publications/PubsFIPS.html.

121. *SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*. 2001 Retrieved 30/3/2012]; Available from: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

122. *GUIDELINE FOR THE USE OF ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES*. 1994 Retrieved 30/3/2012]; Available from: http://csrc.nist.gov/publications/fips/fips190/fip190.txt.

123. *Personal Identity Verification (PIV) of Federal Employees and Contractors*. 2006 Retrieved 30/3/2012]; Available from: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

124. *Network / Perimeter / Wireless - Wireless (Smartphone/Tablet)*. 2012 Retrieved 30/3/2012]; Available from: http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html.

125. *DoD Wireless Smartphone Security Requirements Matrix - Version 3.5*. 2011 Retrieved 30/3/2012]; Available from: http://iase.disa.mil/stigs/downloads/pdf/u_dod_smartphone_email_system_security_req_matrix_v3r5_20110121.pdf.

126. Kilduff, S. and S. McCarey. *Architectural Vision - ICT Mobility - Version 1.1*. 2010 Retrieved 30/3/2012]; Available from: http://intranet.defence.gov.au/_comweb/sites/OBJView.asp?ID=af6642346.

127. Moog, A. *eCryptfs is a POSIX-compliant enterprise cryptographic filesystem for Linux*. 2008 Retrieved 29/6/2012]; Available from: https://launchpad.net/ecryptfs.

128. *Z800 3DVisor*. 2012 Retrieved 5/4/2012]; Available from: http://www.3dvisor.com/.

129. Parviz, B., S. Lee, and S. Thrun. *Project Glass*. 2012 Retrieved 5/4/2012]; Available from: https://plus.google.com/111626127367496192147/posts#111626127367496192147/posts.

130. Beaumont, M., C. North, and J. Green, *Digital Video Guard*. 2009, Defence Science and Technology Organisation (DSTO-TN-0863).

Page classification: UNCLASSIFIED

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION **DOCUMENT CONTROL DATA**	1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE Using Mobile Platforms for Sensitive Government Business	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION) Document (U) Title (U) Abstract (U)
4. AUTHOR(S) Samuel Chenoweth	5. CORPORATE AUTHOR DSTO Defence Science and Technology Organisation PO Box 1500 Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER DSTO-GD- 0722	6b. AR NUMBER AR- 015-497	6c. TYPE OF REPORT General Document	7. DOCUMENT DATE January 2013

8. FILE NUMBER 2012/1143628/1	9. TASK NUMBER 07/012	10. TASK SPONSOR DSD	11. NO. OF PAGES 66	12. NO. OF REFERENCES 130

DSTO Publications Repository http://dspace.dsto.defence.gov.au/dspace/	14. RELEASE AUTHORITY Chief, Command, Control, Communications and Intelligence Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS

Mobile computing, Mobile communications, Information security, Communications security

19. ABSTRACT

Mobile platforms such as smartphones are becoming increasingly popular for both personal and commercial use. When the data being stored and transmitted by these devices is sensitive this can introduce a host of security issues, some of which are discussed in this report. A summary is provided of existing practices for the use of mobile devices with sensitive information, in both governmental and business contexts, and emerging technologies for improving security are reviewed. Finally, some recommendations are offered for policymakers interested in increasing the role that mobile devices are allowed to play within the Australian Public Service and elsewhere.

Page classification: UNCLASSIFIED